



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

TABLE OF CONTENTS

- 1. THE EMERGING SUB-PRIME LENDING SCANDAL AND STRATEGIC APPROACHES TO CLAIMS FOR COVERAGE**
- 2. CYBER LIABILITY: UNDERSTANDING TECHNOLOGY LOSSES IN AN AGE OF E-COMMERCE**
- 3. A CHANGE IN CLIMATE: THE CHILLING EFFECT OF GLOBAL WARMING EXPOSURES**
- 4. PRESERVATION AND E-DISCOVERY FROM A LITIGATION AND RISK MANAGEMENT PERSPECTIVE**



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

***THE EMERGING SUB-PRIME SCANDAL and
STRATEGIC APPROACHES TO CLAIMS FOR
COVERAGE***

Robert J. Re, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

I. OVERVIEW

Today's mortgage market has separated into two segments: the prime market and the sub-prime market. The prime market extends loans to the majority of households with average to excellent credit, while the sub-prime market extends more costly loans to households with less financial security and lower credit scores. Ideally, the sub-prime market presents an opportunity to lenders to extend credit to a class of people that normally would not qualify for home loans and expands the opportunity to own a home to a larger segment of the population.

The U.S. housing market of the past few years has led to a staggering number of sub-prime loans. But, this market expansion has come at a significant cost. To justify the heightened risk, lenders often attach significant fees and balloon payments to loans. Although contested by some market analysts, many attribute increasing defaults on home mortgages and a virtual meltdown of the sub-prime industry to these expensive high risk loans. Although certain sub-prime lenders are experiencing significant financial difficulties, including bankruptcy, the sub-prime meltdown is affecting more than just the originators of the loans. Investors, including large banks, hedge funds and insurance companies, are feeling the financial pressure resulting from the failure of the sub-prime market. In the wake of the crisis, Congress is seeking to strengthen laws to combat the often predatory nature of sub-prime loans to prevent increased default rates in the future.

Over the last several months, lawsuits and investigations of many varieties have been filed or threatened, as investors, trustees and homeowners scramble to recoup losses predicated on the decline of the sub-prime market. It is only a matter of time before litigants embroiled in what may prove to be a long and expensive journey turn to the insurance industry in an effort to defray costs. This paper examines the genesis of the sub-prime market problems and provides an overview of the regulation and litigation reaction that is developing, and the potential effect on insurers.

II. BACKGROUND

Sub-prime lending is a general term that refers to the practice of extending credit to borrowers who do not qualify for loans at market interest rates because they exhibit characteristics indicating a significantly higher risk of default due to deficient credit history. Sub-prime lending encompasses a variety of credit and loan instruments, including bank loans, mortgages, and credit cards, among others.

The term "sub-prime" refers not to the interest rate on the loan instrument itself, but to the credit status of the borrower. The credit status or default risk of a borrower may be measured by traditional credit risk measures (credit and repayment history, debt to income levels, etc.) or by alternative measures such as credit scores. The best known and most widely used credit score model in the United States was developed by the Fair Isaac Corporation ("FICO"). The FICO Score is calculated statistically, taking information from a borrower's credit files collected by credit reporting agencies. Based on FICO, credit scores range between 300 to 900, with most

consumers scoring in the 600s and 700s. While there is no official credit profile that describes a sub-prime borrower, most of them have credit scores below 620.¹

Sub-prime lending involves risk not only lenders, but for borrowers as well. Sub-prime borrowers often default on payments, resulting in either higher debt on the loan or credit card, or in some cases, foreclosure proceedings. Lenders, therefore, use a variety of techniques to offset the default risks associated with these loans, most often using higher rates, loan fees and penalty payments.

Sub-prime lending is highly controversial. Opponents have argued that sub-prime lending companies engage in predatory lending practices such as deliberately lending to borrowers who could never meet the terms of their loans, while proponents maintain that the practice extends credit to people who would otherwise not have access to the credit market.²

A. DEFINITIONS

i. SUB-PRIME LOANS

As stated, sub-prime loans are loans offered to borrowers with low credit scores. Due to the credit risk associated with such loans, lenders offset these risks with a higher interest rate compared to equivalent prime loans.

ii. SUB-PRIME CREDIT CARDS

Sub-prime credit cards are given to credit card holders with a deficient credit history. The risk of default is set off with low credit limits and extremely high late payment fees and interest rates. Sub-prime credit card customers are generally not even given a “grace period” to pay late unlike prime credit card customers.

ii. SUB-PRIME MORTGAGES

Sub-prime mortgages are loans made to borrowers unable to qualify under traditional, more stringent criteria because of a limited or blemished credit history. The risks associated with such mortgages are offset by higher rates, prepayment penalties, and/or balloon payments.

Sub-prime mortgages, in particular, have become increasingly popular since the late 1990s, currently totaling \$600 billion and accounting for one-fifth of the U.S. home loan market. Several iterations of sub-prime mortgages have emerged, including Interest-Only Mortgages (allowing borrowers to pay only the interest on the loan for five to ten years); Pick-a-Payment Mortgages (allowing borrowers to choose their monthly payment by making full payments, interest only payments or other minimal payments); and Adjustable Rate Mortgages.

¹ *Sub-prime Mortgages*, BANKRATE.COM, May 1, 2006, <http://www.bankrate.com/brm/green/mtg/basics2-4a.asp?caret=8>.

² *Economic Scene; ‘Irresponsible’ Mortgages have Opened Doors to Many of the Excluded*, Austan Goolsbee, New York Times, March 29, 2007

The most common sub-prime loan is the Adjustable Rate Mortgage (“ARM”). An ARM is a mortgage loan whose interest rate adjusts periodically based on a defined index. In sub-prime mortgages, the interest rate is set at some margin over the index. The adjustable rates transfer part of the interest rate risk from the lender to the borrower, generally allowing borrowers to lower their initial payments. A hybrid ARM is a mortgage with a low “teaser” rate and payments that jump explosively after the first two or three years.³ A common payment scheme for a hybrid ARM is the “2-28” loan, which offers a low, fixed interest rate for the first two years and a higher adjustable rate for the rest of the life of the loan, usually 28 years. Although hybrid ARMs are seen as a way of protecting borrowers who acquire ARMs because it allows borrowers to increase their income during the period of lower payments, many borrowers are unaware of the subsequent rise in their monthly payments when they acquire such a loan.

B. SUB-PRIME MELTDOWN

i. THE BEGINNING: “RATE WAR OF 2004”

The crisis in the sub-prime industry began with what industry analysts refer to as a “rate war” beginning in 2004.⁴ Sub-prime lenders began cutting rates in order to attract a bigger market share of borrowers. Although the low rates attracted both quality and sub-standard borrowers alike, the business plan was not very profitable in light of increasing lenders’ costs imposed by the Federal Reserve.⁵ The result was a “giant game of chicken,” as described by industry analysts,⁶ with lenders trying to increase profits by raising lending rates. To make up for the higher rates, lenders began to compete for customers by relaxing underwriting standards.⁷ The industry’s game of chicken resulted in several sub-prime lenders declaring bankruptcy beginning in late 2006, including ResMae Mortgage, Mortgage Lenders Network USA, and OwnIt Mortgage Solution.⁸

ii. DOMESTIC FALLOUT: BANKRUPTCIES AND STOCK MARKET DOWNFALLS

By early 2007, various lenders reported troubles in their sub-prime portfolios.⁹ HBC, for example, announced it was setting aside 20% more money than previously estimated to cover

³ Les Christie, *Sub-prime Lenders Push Back*, CNNMONEY.COM, Mar. 22, 2007, http://money.cnn.com/2007/03/22/real_estate/sub-prime_lenders_deny_responsibility/index.htm?postversion=2007032218.

⁴ Peter Coy, *Why Sub-prime Lenders are in Trouble*, BUSINESS WEEK, Mar. 2, 2007, available at http://www.businessweek.com/bwdaily/dnflash/content/mar2007/db20070302_477856.htm?chan=top+news_top+news+index_businessweek+exclusives (quoting Michael Youngblood, head of asset-backed securities research at Friedman, Billings, Ramsey Group (FBR)).

⁵ *Id.*

⁶ *Id.* (quoting Robert Lacoursiere, Banc of America Securities (BAC) analyst).

⁷ *Id.*

⁸ Justin Bachman & Sonja Ryst, *A Painful Hiss from the Sub-prime Balloon*, BUSINESS WEEK, Feb. 22, 2007, available at http://www.businessweek.com/bwdaily/dnflash/content/feb2007/db20070221_387085.htm.

⁹ Maya Roney, *Sub-prime Time Bomb*, BUSINESS WEEK, Feb. 9, 2007, available at http://www.businessweek.com/bwdaily/dnflash/content/feb2007/db20070206_488329.htm.

bad loans in 2006, and watched its stock drop by 3%.¹⁰ New Century Financial, the second largest sub-prime lender in the world, restated results of the first three quarters of 2006 to report a 30% loss in stock price, as well as an expected loss for the fourth quarter. Countrywide Financial's ("CFW") stock fell by 2% and Accredited Home Lenders Holding's ("LEND") was down 7%. Recently, European shares declined.¹¹ Lehman Brothers Holdings Inc. analysts predict that European investment banks will take a 'material hit' to earnings from the fallout of rising U.S. sub-prime-mortgage defaults.¹² Deutsche Bank AG and Credit Suisse Group were downgraded and had their share price estimates cut.

In late February 2007, news from the sub-prime industry looked bleak, with more bankruptcies and other losses being reported everyday. Novastar Financial reported a quarterly loss and stated that it may not have any taxable income until 2011.¹³ Mortgage Lenders Network filed for Chapter 11 protection in February 2007 and identified more than 7,000 creditors with debts of more than \$100 million each.¹⁴ New Century filed for Chapter 11 Bankruptcy on April 2, 2007.¹⁵ In July, Bear Stearns announced that assets in the hedge fund were essentially worthless.¹⁶ On August 6, American Home filed for Chapter 11 bankruptcy-court protection,¹⁷ while on August 22, First Magnus Financial Corporation, one of the largest independent American mortgage lenders, sought protection.¹⁸ Ameriquest Mortgage, the largest American sub-prime lender, closed its operation while the assets of its parent company, ACC Capital Holdings, were purchased by Citigroup.¹⁹

Some of the bankruptcies referenced were triggered by the withdrawal of financing by large banks, such as Merrill Lynch and J.P. Morgan.²⁰ Typically, sub-prime lenders sell their loans to big banks, which package the loans and sell them as mortgage backed securities to hedge funds and other institutional investors.²¹ During the period it takes for the sales to be processed, banks provide lenders with a "warehouse" in which to store the loans. Warehouse

¹⁰ *Id.*

¹¹ *European Stocks Decline on Worries – Credit-Market Troubles Could Spill Over*, Sarah Turner, Wall Street Journal, September 6, 2007

¹² *Lehmann Sees 'Material Hit' to Europe Investment Banks (Update 3)* by Charles Penty, Bloomberg. Com, September 5, 2007

¹³ Bachman & Ryst, *Painful Hiss*, *supra* note 8.

¹⁴ Lingling Wei & Marie Beaudette, *Mortgage Lenders Network Files for Ch. 11 Bankruptcy Protection*, BOSTON.COM, Feb. 5, 2007, http://www.boston.com/news/local/connecticut/articles/2007/02/05/mortgage_lenders_network_files_for_ch_11_bankruptcy_protection/.

¹⁵ Sonja Ryst and Justin Bachman, *The Sub-prime Story's Latest Chapter: 11*, BUSINESS WEEK, Apr. 3, 2007, http://www.businessweek.com/bwdaily/dnflash/content/apr2007/db20070403_365053.htm?chan=search.

¹⁶ *Barclays May Have Lost Big in Bear Fund: Report*, ABCNEWS.COM, July 21, 2007, <http://abcnews.go.com/Business/wireStory?id=3401582>.

¹⁷ *At Mortgage Banks, 'Going Concerns,' Going, Gone* by Jonathan Weil, Bloomberg.com, August 15, 2007

¹⁸ *Big Mortgage Lender in Chapter 11 filing*, Reuters, New York Times, August 22, 2007

¹⁹ *Ameriquest, a Sub-prime Lender, Is Closing*, Reuters, New York Times, August 31, 2007

²⁰ Alistair Barr, *Big Banks Control Fate of Sub-prime Lenders*, MARKETWATCH, Feb. 16, 2007, <http://www.marketwatch.com/News/Story/big-banks-deciding-fates-troubled/story.aspx?guid={08BF0083-33AD-47C7-9EDC-3AB1085BBE43}>.

²¹ *Id.*

banks keep lenders supplied with sufficient cash to make more loans immediately. In light of the suspect future of sub-prime lenders, however, warehouse banks have begun to ask for higher fees. Other warehouse banks have cut their financing completely, forcing sub-prime lenders to post significant collateral. Moreover, purchasers of loans have begun to exercise their right to send loans back to the originators (i.e., sub-prime lenders) in certain circumstances (if the borrowers fail to make payments within the first few months).

In the wake of the rising mortgage default rates around the country, investors have likewise become concerned about the stability of sub-prime lenders. A lack of financial support from banks has led to financial woes for many sub-prime lenders. Examples of the direct impact a non-supportive bank can have on a sub-prime lender are found in the demise of OwnIt and ResMae. JP Morgan provided warehouse financing to OwnIt and, in November 2006, withdrew almost half of OwnIt's cash after making a margin call and withdrawing its finances.²² In February 2007, Merrill Lynch, the largest buyer of ResMae's loans, asked the company to repurchase \$300 million worth of loans, which triggered a liquidity crisis at ResMae.²³ Both OwnIt and ResMae were forced into bankruptcy as a result.

New investors have tried to keep sub-prime lenders afloat. Following ResMae's bankruptcy, Credit Suisse offered to purchase its assets for \$19 million,²⁴ only to be outbid by Citadel Investment Group, which offered \$22.4 million. Citadel also purchased ResMae loans for \$160 million, 98.5% of their face value.²⁵ Lehman Brothers agreed to fund all of Mortgage Lenders Network's pending loans,²⁶ while Farallon Capital Management provided Accredited Home Lenders with a \$230 million loan.²⁷ Finally, CIT Group and Greenwich Capital Financial products agreed to provide New Century with \$150 million.²⁸ Despite these efforts, the sub-prime industry continues its downward trend.

Most recently, industry analysts have attributed a market slowdown to the sub-prime crisis. In July 2007, an unprecedented number of negative rating actions were taken on sub-prime bonds. Standard & Poors ("S&P") put 612 securities backed by sub-prime mortgages on "Credit Watch negative," while Moody's downgraded 399 securities and placed an additional 32 on review for possible downgrade. S&P took the actions because of high delinquencies stemming from lax underwriting standards.²⁹ These actions caused investors to become worried,

²² Alistair Barr, *Big Banks Control Fate of Sub-prime Lenders*, MarketWatch, Feb. 16, 2007, <http://www.marketwatch.com/News/Story/big-banks-deciding-fates-troubled/story.aspx?guid={08BF0083-33AD-47C7-9EDC-3AB1085BBE43}>.

²³ Barr, *ResMAE*, *supra*.

²⁴ Alistair Barr, *Citadel Buys Bankrupt Sub-prime Lender ResMAE*, MarketWatch, Mar. 6, 2007, <http://www.marketwatch.com/news/story/citadel-buys-bankrupt-sub-prime-lender/story.aspx?guid={69BAF585-B597-46CE-891D-F49B4614A6E7}>.

²⁵ *Id.*

²⁶ *Lehman to Fund Pending Mortgage Lenders network Loans*, MARKET WATCH, Jan. 5, 2007, <http://www.marketwatch.com/news/story/lehman-fund-pending-mortgage-lenders/story.aspx?guid=%7b9B608AD7-35EC-4FA2-954C-E1FD46C3037E%7d&print=true&dist=printTop>.

²⁷ Ryst & Bachman, *Latest Chapter: 11*, *supra* note 15.

²⁸ *Id.*

²⁹ Les Christie, *Rating Agencies to Cut Sub-prime Bond Ratings*, CNNMONEY.COM, July 10, 2007, <http://cnnmoney.printthis.clickability.com/pt/cpt?action=cpt&title=Sub-prime+bond+ratings+to+be+slashed+->

resulting in an overall downturn of the U.S. stock market. In addition, Federal Reserve Chairman Ben Bernanke's grim comments about the continued downfall of the U.S. housing market triggered a market fall.

iii. GLOBAL FALLOUT: FROZEN FUNDS

The sub-prime lending crisis has not exclusively been a domestic problem, as reflected by BNP Paribas, France's largest bank, decision to freeze \$2.2 billion worth of funds on August 9, 2007. BNP cited instability of the U.S. sub-prime mortgage sector as the catalyst for its action,³⁰ stating "[t]he complete evaporation of liquidity in certain market segments of the U.S. securitization market has made it impossible to value certain assets fairly, regardless of their quality or credit rating."³¹

One of the largest banks in Germany, IKB Deutsche Industriebank AG, dropped 18% in the stock market after the bank acknowledged its losses from exposure to the United States sub-prime mortgage market,³² requiring emergency funding. In response, several German banks provided € 3.5 billion to IKB to cover its potential losses.³³ Emergency funding was also provided to the German Landesbank Sachsen Girozentrale in August 2007.³⁴ German prosecutors and public interest groups are keeping a close watch on IKB to discover how the bank was so heavily exposed to the sub-prime market and to determine whether the involvement of German government banks in the loan to IKB constitutes an illegal government subsidy.³⁵

iv. EFFECT ON DOMESTIC HOUSING MARKET

Of obvious concern to homeowners and financial analysts is the impact the rising default rates and the collapse of the sub-prime lending industry will have on the US housing market. Some analysts believe the troubles in the sub-prime lending market will not spread to the housing market because most of the homes purchased with sub-prime mortgages were at the low end of the market.³⁶ However, other experts are more concerned. Michael Simonsen, president and CEO of Altos Research, which studies California and fifteen other U.S. real estate markets, stated that the sub-prime mortgage crisis is "one of the scariest signs" for the U.S. housing

+Jul.+10,+2007&expire=-1&urlID=23000753&fb=Y&url=http://money.cnn.com/2007/07/10/real_estate/Sub-prime-bond-ratings-to-be-slashed/index.htm&partnerID=2200.

³⁰ *Sub-prime Woes Hit BNP Paribas*, CNNMONEY.COM, August 9, 2007,

http://money.cnn.com/2007/08/09/news/international/bnp_sub-prime.reut/?postversion=2007080910.

³¹ *Id.*

³² Robert Daniel, *IKB Stock Slumps After Warning on Sub-prime Impact*, MARKETWATCH, July 30, 2007,

<http://www.marketwatch.com/news/story/german-lender-ikb-slumps-us/story.aspx?guid={78C7C9A1-8669-4157-9E76-5213F1634C46}>.

³³ John O'Donnell, *IKB Sub-prime Shockwaves Continue to Rock Germany*, SIGNONSANDIEGO.COM, Aug. 3, 2007,

<http://www.signonsandiego.com/news/business/20070803-0641-ikb-rescue-.html>.

³⁴ *Lehmann Sees 'Material Hit' to Europe Investment Banks (Update 3)* by Charles Penty, Bloomberg. Com, September 5, 2007

³⁵ *Id.*; *German Prosecutors to Look at IKB's Sub-prime-Related Collapse*, INT'L HERALD TRIBUNE, Aug. 3, 2007,

<http://www.iht.com/articles/ap/2007/08/03/business/EU-FIN-COM-Germany-US-Sub-prime-Woes.php>.

³⁶ Bachman & Ryst, *Painful Hiss*, *supra* note 8.

market.³⁷ Federal Reserve Chairman Ben Bernanke recently told Congress that the Federal Reserve believes the housing slowdown will last longer than anticipated.³⁸ Market analysts interpreted his comments on housing as related to the sub-prime mortgage crisis, causing a downward slide in the stock market in July 2007.

Despite the large fallout, some lenders continue to claim that sub-prime mortgage lending has not contributed to the increasing defaults on mortgages around the country. At a recent Senate Banking Committee hearing, Sandy Samuels, an executive with Countrywide Financial, proffered that the majority of hybrid ARMS have not gone through reset (only 20,000 of the 540,000 of the sub-prime loans Countrywide issued are going into default).³⁹ Scott M. Polakoff, COO for the Office of Thrift Supervision, has observed that problems in local economies, especially in Ohio, Pennsylvania, and Michigan, are causing the rising default rates.⁴⁰

III. LITIGATION ISSUES

A. SUMMARY OF PENDING LAWSUITS

The sub-prime lending and mortgage crisis has set off a wave of litigation in 2007. Borrowers have sued lenders. Lenders have sued financial institutions. Financial institutions have sued lenders. Even regulators have looked to the Courts for relief. **See attached Exhibit for a list of filed actions.**⁴¹ Current actions generally fall into three categories: 1) Lender Liability claims brought by originators or bankruptcy trustees against lending banks; 2) U.S. Securities Act claims brought by investors whose mortgage-backed securities have suffered significant losses; and 3) homeowners' claims against mortgage originators, brokers and banks premised on improper lending practices. Allegations include breach of contract, breach of fiduciary duty, violations of U.S. Securities laws, fraud and "aiding and abetting" improper or fraudulent conduct.

i. LENDER LIABILITY CLAIMS

As stated, much of the fallout in the sub-prime market is the result of warehouse banks withdrawal of financing to mortgage loan originators. Because, in many instances, the mortgage originator's only business is the sale of new loans, credit lines and financing from warehouse banks is the lifeblood of the originator's business model. Once the source of funds to the originator stops, so too does the ability of the originator to generate new loans. The result, in many instances, is insolvency for the mortgage originator.

Insolvent originators and Bankruptcy Trustees have begun to file suits against lenders that have terminated credit facilities to originators. These actions may take the form of breach of

³⁷ *Id.*

³⁸ Kristina Cooke, *Bernanke's View, Sub-prime Mess Push Wall St. Down*, ABCNews.com, July 18, 2007, <http://abcnews.go.com/Business/wireStory?id=3390232>

³⁹ Christie, *supra* note 1.

⁴⁰ *Id.*

⁴¹ The list is not exclusive

contract or tort liability. While a breach of contract claim will largely depend on the contract terms and conditions of the agreement between originator and lender, the viability of business tort claims, like breach of fiduciary duty, is less clear. Actions under a theory of breach of fiduciary, for example, are premised on the notion that “[t]he essence of a fiduciary relationship is that one party places trust and confidence in another who is in a dominant or superior position. The fiduciary relationship arises between two persons when one person is under a duty to act for or give advice for the benefit of another on matters within the scope of their relationship.”⁴² “The virtually unanimous rule is that creditor-debtor relationships rarely give rise to a fiduciary duty.”⁴³ “Fiduciary relationships implied in law are premised upon the specific factual situation surrounding the transaction and the relationship of the parties.”⁴⁴ “As aptly noted by the Court of Appeals for the Third Circuit, it ‘would be anomalous to require a lender to act as a fiduciary for interests on the opposite side of the negotiating table,’ because their respective positions are essentially adversarial.”⁴⁵ There is, therefore, a general presumption that the “relationship between lenders and borrowers is conducted at arms-length, and the parties are each acting in their own interest.”⁴⁶

In addition to claims seeking recovery on behalf of mortgage originators, several other contract based claims have been asserted against those same originators. Mortgage loan purchasers, such as investment banks, have sued originators due to the failure to repurchase defaulted loans, as required under certain loan purchase agreements. Fifteen of these claims have been filed by DBSP, Inc. (Deutsche Bank Structured Products), a subsidiary of Deutsche Bank, alone. Moreover, warehouse lenders have asserted breach of contract claims of their own for failure to repurchase early payment default loans. At least 25 such cases have been filed in New York state courts.⁴⁷

ii. SECURITIES ACT CLAIMS

Several lawsuits have been filed against mortgage lending companies or mortgage originators. Claims asserted typically include violation of the Securities Exchange Act of 1934, breach of contract (loan purchase agreements), and violation of laws governing lending practices (e.g., Fair Housing Act and Equal Credit Opportunity Act).

Shareholder claims made under the Securities Exchange Act of 1934 allege that mortgage lending companies issued materially false and misleading statements regarding the company’s business and financial results, leading to artificially inflated stock prices. Lawsuits are premised on the company’s failure to disclose (1) an increasing level of loan delinquencies; and (2) insufficient liquidity. Once true disclosure is made, shareholders argue, stock value rapidly declines, and often leading to a halt in trading.

⁴² F.G. v. MacDonell, 150 N.J. 550, 563-64 (1997).

⁴³ *Id.* at 552 (citations omitted).

⁴⁴ *Ibid.*

⁴⁵ *Id.* at 552 (quoting Paradise Hotel Corp. v. Bank of Nova Scotia, 842 F.2d 47, 53 (3d Cir. 1988).

⁴⁶ *Id.* at 552.

⁴⁷ *Legal Claims Proliferate From Mortgage Meltdown* by Beth Bar, August 22, 2007

Investment banks and others have likewise been sued under the Securities Exchange Act of 1934 for misrepresentation or failure to disclose material facts. Examples of such actions include the following:

- **Credit Suisse**

In 2004, Bankers Life Insurance Co. purchased security certificates from Credit Suisse First Boston (CSFB) collateralized by pools of individual sub-prime mortgage loans on residential real estate. The mortgage loans were serviced and sold by CFBS affiliates and maintained in a trust with Bank of New York as trustee.

The certificates, commonly known as Asset Backed Securities suffered a downgrade commencing in January 2005 due to problems with loan delinquencies. Bankers Life sued Credit Suisse alleging claims of negligent misrepresentation in the prospectus, common law fraud, and breach of fiduciary duty.

- **Bear Stearns**

It has been reported that investors intend to file suit against Bear Stearns alleging misrepresentation in response to the fund revealing in July 2007 that the company's assets were essentially worthless.⁴⁸ Enforcement agencies will assess the lenders' underwriting standards and their risk-assessment oversight for ensuring compliance with consumer protection laws and intend to initiate corrective or enforcement action as necessary based upon the results of the studies.⁴⁹

- **Moody's CFO**

The CFO and executive vice president of Moody's has been sued by an individual investor under the Securities Exchange Act for 1934 for misrepresentation and failure to disclose that the company assigned excessively high ratings to bonds backed by risky sub-prime mortgages. Although there typically is no duty to disclose in a normal lender-borrower relationship, a court may imply a duty to disclose in cases of egregious breaches of good faith and fair dealing.⁵⁰

Claims of fraud and "aiding and abetting fraud" are also quite appealing to plaintiffs, as each presents the opportunity to recover punitive damages. Legal fraud consists of the material misrepresentation of a fact, made with the intention that the other party rely [on the misstatement], resulting in detrimental reliance by that party⁵¹ and, therefore, is often difficult to

⁴⁸ *Barclays May Have Lost Big in Bear Fund: Report*, ABCNews.com, July 21, 2007, <http://abcnews.go.com/Business/wireStory?id=3401582>.

⁴⁹ Federal and State Agencies Announce Pilot Project to Improve Supervision of Sub-prime Mortgage Lenders, *supra* note 117.

⁵⁰ *Id.* at 557-58.

⁵¹ *Id.* at 551 (quoting *Jewish Center of Sussex County v. Whale*, 86 N.J. 619, 624 (1981)).

prove. However, “silence in the face of a duty to disclose may constitute a fraudulent concealment.”⁵² Thus, the exposure remains a real threat.

iii. Consumer Actions

In addition to claims asserted by commercial entities concerning secondary market issues, various claims have been asserted on behalf of consumers against mortgage lenders for misrepresentation and failing to disclose loan terms and fees. Notably, several racially-premised discrimination actions have been filed, including:

- Wells Fargo sued by African-American borrowers for violations of the Fair Housing Act.
- Four African American homeowners sued Countrywide Financial Corp. alleging racial discrimination in the company’s lending practices and are currently seeking class action status.⁵³ The plaintiffs accused Countrywide of marking up interest rates or tacking on fees to loans to African Americans after agreeing to lend based on criteria such as credit histories or home values.
- The NAACP has sued 14 lenders in a class action alleging violations of the Fair Housing Act, Equal Credit Opportunity Act and Civil Rights Act.⁵⁴ The NAACP bases its allegations on studies by the Center for Responsible Lending and National Community Reinvestment Coalition which state that African Americans are more likely to be issued sub-prime and high rate loans than Caucasian borrowers. The NAACP has charged that the lending industry had a long history of discrimination and has alleged that the fees associated with the loans are not properly disclosed to borrowers.

While by no means an exhaustive list of consumer claims, the aforementioned matters are indicative of types of predatory lending actions that have, and will continue to be, asserted on behalf of consumers. Such claims have also exposed purported shortfalls in the regulation of sub-prime lending and related issues.

⁵² *Id.* at 551.

⁵³ Jonathon Stempel, *Countrywide Sued for Racial Bias in Mortgage Loans*, ABCNews.com, July 12, 2007, <http://abcnews.go.com/Business/IndustryInfo/wireStory?id=3372236>.

⁵⁴ NAACP press release, July 11, 2007

<http://www.naacp.org/get-involved/activism/alerts/110aa-2007-7-11/index.htm>

NAACP Sub-prime Discrimination Suit, MortgageNewsDaily, July 16, 2007,

http://www.mortgagenewsdaily.com/7162007_NAACP_Sub-prime_Lawsuit.asp (providing a link to the complaint filed in the class action suit).

IV. REGULATING SUB-PRIME LENDING

A. FEDERAL REGULATION

In reaction to the sub-prime mortgage crisis, federal regulators have been criticized for a lack of regulation in the sub-prime area. Questions abound concerning whether sub-prime lending requires stricter federal regulations to prevent predatory lending business.

Currently, only a minority of sub-prime lenders are regulated by federal law and monitored by the Federal Reserve Board of Governors, members of which include the twelve federal reserve banks, national chartered banks commencing business in the United States; and certain state chartered banks. Moreover, in 2005, only about one-quarter of sub-prime loans originated from such federally regulated lenders. The remaining book of sub-prime business originated sources operating with limited federal regulations.⁵⁵ Although the Federal Reserve has authority under the Home Ownership and Equity Protection Act of 1994 (“HOEPA”) to regulate all sub-prime lenders, it has, in the past, been hesitant to use this power and has instead left regulation to the states.

This is not to suggest that there are no federal regulations or mechanisms in place to address concerns over lending activities. Indeed, many such regulations exist for the specific goal of preventing predatory lending. These regulations include the following:

- **Truth in Lending Act and Home Ownership and Equity Protection Act**

Although not specifically anti-predatory in nature, the Federal Truth in Lending Act requires certain disclosures of APR and loan terms.⁵⁶

In 1994, § 32 of the Truth in Lending Act, entitled the Home Ownership and Equity Protection Act of 1994 (HOEPA), was created. This law is devoted to identifying certain high-cost, potentially predatory mortgage loans and reining in their terms. HOEPA is implemented by Regulation Z⁵⁷ which sets forth further obligations. Open ended or closed ended home equity loans under which the total points and fees paid by the consumer exceed the greater of 8% of the loan or \$400.⁵⁸ HOEPA and TILA, however, do not apply to home purchase loans.⁵⁹

Under HOEPA and TILA, creditors must disclose certain items to a borrower when issuing a home mortgage. Lenders must affirmatively represent to the borrowers that they are not required to complete the agreement merely because they have signed loan application.⁶⁰ Lenders must also inform borrowers that

⁵⁵ *Banking Regulators to Increase Scrutiny of Sub-prime Lenders*, N.Y. TIMES, July 18, 2007, at C2.

⁵⁶ 15 U.S.C. §1601 et. seq.

⁵⁷ 12 C.F.R. pt. 226.

⁵⁸ 15 U.S.C. §1602(aa); 12 C.F.R. §226.32(a)(1).

⁵⁹ 12 C.F.R. §226.32(2).

⁶⁰ 15 U.S.C. §1639(a)(1)(A); 12 C.F.R. §226.32(c)(1).

foreclosure can result for a failure to meet obligations under the loan.⁶¹ In addition, lenders must disclose the annual percentage rate,⁶² the amount of a regular monthly payment, and the amount of increase in the monthly payments.⁶³ For variable rate transactions, lenders must additionally disclose that the monthly payment may increase and the amount of the maximum payment.⁶⁴

Finally, loans subject to TILA and HOEPA can not contain the following terms:⁶⁵

2. balloon payments for loans with terms of less than 5 years
3. negative amortization
4. advance payments
5. increased interest rate after default
6. rebates calculated in a method less favorable than HUD's actuarial method
7. prepayment penalties
8. due on demand clause

- **Real Estate Settlement Procedures Act (RESPA)**

The RESPA⁶⁶ sets procedures for lending practices and closing and settlement procedures for the purpose of ending unnecessary costs and minimizing difficulties of purchasing housing. However, the act is binding only on lending in federally related mortgage transactions.⁶⁷

- **Home Mortgage Disclosure Act (HMDA)**

The HMDA⁶⁸ provides the public with loan data in order to determine whether financial institutions are meeting the community's housing needs, assist public officials in the distribution of public investment, and identify discriminatory lending practices.⁶⁹ HMDA applies to financial institutions as defined under the HMDA.⁷⁰

⁶¹ *Id.* §1639(a)(1)(B); 12 C.F.R. §226.32(c)(1).

⁶² *Id.* §1639 (a)(2); 12 C.F.R. §226.32(c)(2).

⁶³ 12 C.F.R. §226.32(c)(3).

⁶⁴ *Id.* §226.32(c)(4).

⁶⁵ *Id.* §226.32(d).

⁶⁶ 12 U.S.C. §2601 et seq.

⁶⁷ 12 U.S.C. §2602

⁶⁸ 12 U.S.C. §2801 et seq.

⁶⁹ 12 C.F.R. §203.1(b).

⁷⁰ *Id.* §203.1(c).

- **Fair Housing Act (FHA)**⁷¹

FHA was enacted in 1968 to prohibit discrimination in real estate transactions. FHA states, “[i]t shall be unlawful for any person or other entity whose business includes engaging in residential real estate-related transactions to discriminate against any person in making available such a transaction, or in the terms or conditions of such a transaction, because of race.”⁷²

- **Equal Credit Opportunity Act (ECOA)**⁷³

ECOA was enacted in 1974 to prohibit discrimination in the issuing of credit. ECOA states, “[i]t shall be unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction...on the basis of race.”⁷⁴

- **Federal Deposit Insurance Act (FDIA)**⁷⁵

FDIA established the Office of Comptroller of the Currency, Guidelines for Residential Mortgage Lending Practices, designed to prevent predatory lending practices.⁷⁶

- **Federal Deposit Insurance Corporation (FDIC) Statements of Policy**⁷⁷

The FDIC issued Interagency Guidance on sub-prime lending as early as March 1, 1999 that state “[i]nstitutions that originate or purchase sub-prime loans must take special care to avoid violating fair lending and consumer protection laws and regulations. Higher fees and interest rates combined with compensation incentives can foster predatory pricing or discriminatory ‘steering’ of borrowers to sub-prime products for reasons other than the borrower’s underlying creditworthiness.”

⁷¹ 42 U.S.C. §3601.

⁷² *Id.* §3605.

⁷³ 15 U.S.C. §1691 *et seq.*

⁷⁴ *Id.* §1691(a)(1).

⁷⁵ 12 U.S.C. §1831.

⁷⁶ 12 C.F.R. pt. 30, Appendix C.

⁷⁷ 5000 – FDIC Statements of Policy “Interagency Guidance on Sub-prime Lending”, March 1, 1999

- **Federal Trade Commission Act (FTCA)** ⁷⁸

Under the FTCA, the Office of Thrift Supervision (OTS)⁷⁹ is responsible for promulgating regulations to prevent unfair or deceptive acts or practices by “savings associations.”⁸⁰ Pursuant to the FTC, OTS is given the authority to define specific acts or practices as unfair or deceptive and impose measures to prevent unfair or deceptive practices.⁸¹ The following are defined as unfair or deceptive practices for the purposes of the FTC:

(1) A cognovit or confession of judgment (for purposes other than executory process in the State of Louisiana), warrant of attorney, or other waiver of the right to notice and the opportunity to be heard in the event of suit or process thereon;

(2) An executory waiver or a limitation of exemption from attachment, execution, or other process on real or personal property held, owned by, or due to the consumer, unless the waiver applies solely to property subject to a security interest executed in connection with the obligation;

(3) An assignment of wages or other earnings, unless:

- (i) The assignment by its terms is revocable at the will of the debtor;
- (ii) The assignment is a payroll deduction plan or preauthorized payment plan, commencing at the time of the transaction, in which the consumer authorizes a series of wage deductions as a method of making each payment; or
- (iii) The assignment applies only to wages or other earnings already earned at the time of the assignment;

(4) A nonpossessory security interest in household goods other than a purchase-money security interest.⁸²

⁷⁸ 15 U.S.C. §41-58.

⁷⁹ The FTC refers to the OTS’s predecessor agency, the Federal Home Loan Bank Board (FHLBB). However, Congress transferred the rulemaking power of FLHBB to OTS. 12 U.S.C. §1462a(e).

⁸⁰ 15 U.S.C. §57a(f)(1). The Federal Reserve Board is given the power to promulgate regulations for banks, OTS for “savings associations,” and the National Credit Union Administration Board for national credit unions. *Id.*

⁸¹ 15 U.S.C. §57a(f)(1).

⁸² 12 C.F.R. §535.2.

Home Owners Loan Act (HOLA)⁸³

HOLA gives OTS the authority to proscribe regulations governing unfair or deceptive practices that cover a broader category of institutions within the savings and loan association structure than the FTC Act. Under HOLA, OTS has the authority to regulate subsidiaries owned in whole or in part by a savings association, savings and loan holding companies other than a bank and their subsidiaries, and certain service providers.⁸⁴ OTS uses this rulemaking authority to supplement that granted to it under the FTC Act. OTS has used this rulemaking authority to promulgate its Advertising Rule, which prohibits savings associations from engaging in deceptive advertising, and its Nondiscrimination Rule, which prohibits discrimination in areas not covered by the federal fair lending laws.⁸⁵

Moreover, the Department of Justice and the Department of Housing and Urban Development (“HUD”) are empowered under 12 U.S.C. §1818 to combat predatory lending. The enforcement power applies to savings and loan holding companies.⁸⁶ Section 1818 can require an institution to make restitution or provide reimbursement for a loss if the practice resulted in unjust enrichment of the lender or involved a reckless disregard for the law.⁸⁷ The enforcement power also includes the authority to restrict the growth of the institution, dispose of the loan or asset involved in the illegal practice, rescind agreements or contracts, employ qualified officers, or take any other necessary action.⁸⁸

B. STATE REGULATION

At least twenty-four states have passed anti-predatory lending laws.⁸⁹ Arkansas, Georgia, Illinois, Massachusetts, North Carolina, New York, New Jersey, New Mexico and South Carolina are among those states considered to have the strongest laws. State anti-predatory lending laws usually extend the protection afforded by HOEPA.

State law usually describes one or more classes of “high-cost” or “covered” loans, which are defined by the fees charged to the borrower at origination or the APR. While lenders are not prohibited from making “high-cost” or “covered” loans, a number of additional restrictions are

⁸³ 12 U.S.C. §1461 et seq.

⁸⁴ *Id.* §1462a(b)(2), 1463(a), 1464(a), 1464(d)(7)(A), 1467a(b), 1467a(g).

⁸⁵ 12 C.F.R. §528.2.

⁸⁶ 12 U.S.C. §1818(9).

⁸⁷ *Id.* §1818(6)(A).

⁸⁸ *Id.* §1818(6)(B-F).

⁸⁹ Giang Ho & Anthony Pennington-Cross, *The Impact of Local Predatory Lending Laws* (Federal Reserve Bank of St. Louis, Working Paper Series, 2005), available at <http://www.newhomebuyer.org/home/finance/predatorylendinglaws.pdf>. The list of states with anti-predatory lending laws used in this paper includes the following 24 states: Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Kentucky, Maine, Maryland, Massachusetts, Nevada, New Jersey, New Mexico, New York, North Carolina, Ohio, Oklahoma, Pennsylvania, south Carolina, Texas, Utah, Wisconsin. *Id.* at 16.

placed on these loans, and the penalties for noncompliance can be substantial. Prepayment penalties are often prohibited in the early life of the loan and balloon payments can be limited in size.⁹⁰ An examination of New York’s regulatory scheme is instructive.

New York State’s anti-predatory lending law took effect on April 1, 2003. The law applies to “high cost home loans.”

“Home loan” means a home loan, including an open-end credit plan, other than a reverse mortgage transaction, in which:

- (i) The principal amount of the loan does not exceed the lesser of:
 - (A) conforming loan size limit for a comparable dwelling as established from time to time by the federal national mortgage association; or
 - (B) three hundred thousand dollars;
- (ii) The borrower is a natural person;
- (iii) The debt is incurred by the borrower primarily for personal, family, or household purposes;
- (iv) The loan is secured by a mortgage or deed of trust on real estate upon which there is located or there is to be located a structure or structures intended principally for occupancy of from one to four families which is or will be occupied by the borrower as the borrower's principal dwelling; and
- (v) The property is located in this state.⁹¹

A “high cost” loan is one which exceeds one or more of the following thresholds:

- If it is a first-lien mortgage, the annual percentage rate of the home loan exceeds 8% of the yield on treasury securities having comparable maturities;
- If it is a junior-lien mortgage, the annual percentage rate of the loan exceeds 9% of the yield on treasury securities having comparable maturities;
- If the loan is a conventional loan for more than \$50,000, and total “points and fees” exceed 5% of the loan;
- If the loan is an FHA or VA loan for more than \$50,000 and the total “points and fees” exceed 6% of the loan; or
- If the loan is less than \$50,000, and the total “points and fees” exceed 6% of the loan or \$1,500, whichever is greater.⁹²

⁹⁰ *Id.*

⁹¹ N.Y. BANKING LAW §6-1 1.(e) (McKinney 2007).

⁹² *Id.* §6-1 1(g).

New York's anti-predatory lending law applies the following restrictions to define "high cost home loans":

- No call provisions
- No balloon payments within the first fifteen years of the loan
- No negative amortization
- No interest rate increase in response to default
- No limitations on advance payments
- No modification or deferral fees
- No oppressive mandatory arbitration
- No financing of insurance
- No "loan flipping"
- No refinancing of special mortgages
- No lending without regard for a borrower's ability to repay the loan
- No lending without counseling disclosure and a list of counselors
- No financing of points and fees in an amount which exceeds three percent of the loan amount
- Lender can not pay a home improvement contractor with proceeds from a high cost loan unless it is done through certain mechanisms which protect the borrower
- No kickbacks to mortgage brokers
- No points and fees are to be charged when a lender refinances its high cost loan with another high cost loan
- No encouragement of default.⁹³

A borrower can bring a private action against a lender for violation of New York's anti-predatory loan laws within six year of the violation and the lender can be found liable to the borrower for actual and statutory damages and attorney's fees.⁹⁴ In addition, New York's Attorney General and Superintendent can enforce the provisions of this law.⁹⁵

State bank regulators are beginning to enforce lending practice regulations in an effort to protect consumers within its borders. For example, Connecticut Banking Commissioner Howard Pitkin issued a cease and desist order in January alleging that Mortgage Lenders failed to satisfy its funding commitments to 93 borrowers in state and 1,400 in other states. Mortgage Lenders could be fined up to \$7 million.⁹⁶

⁹³ *Id.* §6-12.

⁹⁴ *Id.* §6-16-8.

⁹⁵ *Id.* §6-15.

⁹⁶ Wei & Beaudette, *supra* note 14.

C. NEW STEPS IN REGULATING THE INDUSTRY

On June 29, 2007, the Federal Reserve, comptroller of the Currency, the Federal Deposit Insurance Corporations, the Office of Thrift Supervision, and the National Credit Union Administration, issued a Statement on Sub-prime Mortgage Lending,⁹⁷ which contains guidelines on “how institutions can offer certain adjustable rate mortgage (ARM) products in a safe and sound manner, and in a way that clearly discloses the risks that borrowers may assume.”⁹⁸ One important aspect of the guidelines instructs lenders to base a borrower’s approval on the loan terms after the rate resets higher.⁹⁹ The guidelines also state that, because sub-prime lending involves a greater credit risk, lenders should require that a borrower’s assets, income, and liabilities should be verified unless there are mitigating circumstances.¹⁰⁰ Although this is an “important first step,”¹⁰¹ the federal government does not have control over all sub-prime lenders and it is unclear if state regulators will adopt these policies.

On July 12, 2007, Alabama Representative and Republican head of the U.S. House Financial Services Committee, Senator Spencer Bachus, introduced the Fair Mortgage Practices Act.¹⁰² The bill seeks “to increase uniformity, reduce regulatory burden, enhance consumer protection, and reduce fraud” in the sub-prime mortgage industry.¹⁰³ The bill, if enacted, would require lenders to be licensed,¹⁰⁴ set licensing standards for mortgage lenders,¹⁰⁵ and catalog those lenders in a national database.¹⁰⁶ Lenders who had a lending license or similar license revoked in the past five years or been convicted of a felony would not be eligible for a license under the bill.¹⁰⁷ The applicant must also demonstrate financial responsibility and good character, have completed an approved education course, and pass a written test.¹⁰⁸ Lenders would also have to submit to a criminal background check and fingerprinting,¹⁰⁹ and those convicted of fraud would not qualify for a license under the proposed standards.

The bill would amend TILA to require disclosure of certain information for all mortgages secured by the borrower’s principal dwelling.¹¹⁰ Like the previously mentioned Statement on Sub-prime Mortgage Lending, the bill would require lenders to evaluate a borrower’s ability to

⁹⁷ Floyd Norris, *Regulators Set Final Rules to Limit Sub-prime Mortgage Lending*, N.Y. TIMES, June 30, 2007 at C2.

⁹⁸ Statement on Sub-prime Mortgage Lending, 72 Fed. Reg. 37,569, 37,569 (July 10, 2007).

⁹⁹ *Id.* at 37,573.

¹⁰⁰ *Id.*

¹⁰¹ Norris, *supra* note 97 (quoting Michael D. Calhoun, president of the Center for Responsible Lending).

¹⁰² *Republican Lawmaker Introduces Sub-prime Legislation*, CNBC.COM, July 12, 2007,

<http://www.cnbc.com/id/19730997>; Fair Mortgage Practices Act of 2007, H.R. 3012, 110th Cong. §§101-701 (1st Sess. 2007).

¹⁰³ H.R. 3012, §101.

¹⁰⁴ *Id.* §103.

¹⁰⁵ *Id.* §104(b)

¹⁰⁶ *Id.* §106.

¹⁰⁷ *Id.* §104(b)(1-2).

¹⁰⁸ *Id.* §104(b)(3-5).

¹⁰⁹ *Id.* §104(a).

¹¹⁰ *Id.* §201.

repay the loan¹¹¹ and prohibits penalties against homeowners that refinance into a lower cost loan.¹¹²

The Office of Thrift Supervision issued the Prohibited Consumer Credit Practices rule over 20 years ago.¹¹³ In August 2007, OTS published an Advanced Notice of Proposed Rulemaking to solicit comments on how to promulgate additional regulation to protect consumers from predatory lending practices.¹¹⁴ OTS is considering a variety of sources to gain insight into how to remodels its consumer protection regulations, including agency guidelines, including that of FTC, and state laws.¹¹⁵ OTS is also considering using regulations targeted at specific practices such as credit card lending and residential mortgage lending.¹¹⁶

Finally, the Federal Reserve, the Office of Thrift Supervision, the Federal Trade Commission and two associations of state regulators, the Conference of State Bank Supervisors and the American Association of residential Mortgage Regulators are set to cooperate in a pilot program to conduct consumer-protection compliance reviews of selected non-depository sub-prime lenders.¹¹⁷

As demonstrate above, regulators have a wide variety of resources available to them to investigate, prosecute and collect from individuals or entities involved in prohibited lending practices. Just how far regulators push, or where its investigations might lead, remains uncertain at this time.

V. CONCLUSION

While a substantial amount of litigation and regulation activity has already ensued as a result of the declining sub-prime market, its effect on insurers and reinsurers is still somewhat of an unknown. It is likely that litigants will look to defray litigation costs and exposure by turning to professional liability and directors and officers' insurers for coverage. The costs in responding to government investigations, for example, may also prove to be a source of exposure to insurers. An expansion to claims against auditing and accounting firms remains a distinct possibility as well.

¹¹¹ *Id.* §412.

¹¹² *Id.* §411.

¹¹³ 50 Fed. Reg. 77440 (March 1, 1984).

¹¹⁴ 72 Fed. Reg. 43,570 (Aug. 6, 2007).

¹¹⁵ *Id.* at 43,573-74.

¹¹⁶ *Id.* at 43,574-75.

¹¹⁷ Press Release, The Federal Reserve Board, Federal and State Agencies Announce Pilot Project to Improve Supervision of Sub-prime Mortgage Lenders (July 17, 2007), *available at* <http://www.federalreserve.gov/BoardDocs/press/bcreg/2007/20070717/default.htm>.

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

	<u>Page</u>
I. OVERVIEW	2
II. BACKGROUND	2
A. DEFINITIONS	3
B. SUB-PRIME MELTDOWN	4
III. LITIGATION ISSUES	8
A. SUMMARY OF PENDING LAWSUITS	8
IV. REGULATING SUB-PRIME LENDING	12
A. FEDERAL REGULATION	12
B. STATE REGULATION	16
C. NEW STEPS IN REGULATING THE INDUSTRY	19
V. CONCLUSION	20



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

***CYBER LIABILITY: UNDERSTANDING
TECHNOLOGY LOSSES IN AN AGE OF
E-COMMERCE***

**Suzanne C. Midlige, Esq.
William J. Hoffman, Esq.**

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

I. INTRODUCTION..... 1

 A. The Emergence of Cyber Risks 1

 B. Storage of consumer data as a “cyber-risk” 5

 C. Storage of a company’s own proprietary or essential business information as a
 “cyber-risk” 6

 D. Data Notification Laws 7

II. INSURANCE COVERAGE FOR CYBER-RISKS UNDER A TYPICAL
 COMPREHENSIVE GENERAL LIABILITY POLICY 12

 A. Data held to be “intangible” 14

 B. Data held to be “tangible” 18

 C. Potentially Applicable Exclusions under Coverage A 25

 D. Personal and Advertising Injury Coverage for Cyber-Risk Claims..... 30

 E. Potential Coverage under Directors’ and Officers’ and Errors and
 Omissions Policies 34

III. THE DEVELOPMENT OF CYBER-RISK INSURANCE AND CYBER-RISK
 MANAGEMENT 35

 A. Cyber-risk insurance 35

 B. Risk management guidelines..... 39

IV. CONCLUSION..... 44

I. INTRODUCTION AND BACKGROUND

A. *The Emergence of Cyber Risks*

In today's digital world, where electronic transactions are processed with lightning speed and where companies both large and small typically maintain confidential or proprietary data in electronic format, both the inadvertent loss of data and the theft of data by a new breed of thief -- the cyber-criminal -- pose an ever-increasing risk for unwary businesses. Just ask one of America's largest retail conglomerates, The TJX Companies, Inc. ("TJX"), parent company of TJ Maxx, Marshalls and several other discount retailers operating in the United States and abroad.

Over an 18-month period between July 2005 and December 2006, sophisticated computer hackers stole approximately 46 million credit and debit card numbers belonging to TJX customers in the United States, Canada and Puerto Rico. *See* Joseph Pereira, *Breaking the Code: How Credit Card Data Went Out Wireless Door*, *The Wall Street Journal* (May 4, 2007). Other estimates have put the number as high as 200 million card numbers stolen from four years' worth of electronic data. *Id.* To make matters even worse, the hackers also stole the social security numbers, military identification numbers and driver's license numbers of approximately 450,000 TJX customers -- the type of information that is a veritable goldmine for identity thieves. *Id.*

TJX has been hit with several consumer class action lawsuits as a result of the breach of its computer network, as well as various investigations from state attorneys' general and a Congressional inquiry. As part of a proposed class action settlement recently announced in late September, TJX has agreed to, among other things, pay the cost of three years' worth of credit monitoring and identity theft insurance to the 450,000

or so customers whose personal information is believed to have been stolen. *See* TJX Settlement Filing (September 22, 2007).¹ While the specific cost of credit monitoring is not set forth in the proposed agreement, the ultimate cost to TJX could be quite significant. Assuming, for example, that the cost of three years of credit monitoring amounts to \$300 per person, the cost to TJX would be \$67,500,000 if only *half* of the 450,000 individual consumers had their credit reports monitored for fraudulent activity.²

That cost is in addition to the \$6.5 million in legal fees TJX has agreed to pay to plaintiffs' class counsel, the \$30 store vouchers it has agreed to provide to customers who made non-cash purchases during the relevant period, as well as other significant costs the company will incur under the terms of the proposed settlement. *Id.* In its earnings report for the second quarter of 2007, TJX took a \$118 million after-tax charge for the quarter to cover current and potential costs arising from the theft, and may record an additional \$21 million in non-cash charges in the future. *See* Walaika Haskins, *TJX Asked Too Much, Protected Too Little, Say Canadian Officials*, CRMBuyer (September 26, 2007) available online at <http://www.ectnews.com>. In addition, estimates are that TJX will spend an estimated total of \$125 million on network security improvements as a result of the breach. *Id.*

TJX's experience is not unique, however. Choice Point, Inc. ("Choice Point"), a consumer data broker, experienced a security breach in 2005 that affected more than 140,000 people in all fifty states. Mary J. Hildebrand and Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance*

¹ The TJX settlement filing is available online at <http://storefrontbacktalk.com/story/092207TJXfiling.php>.

² Based on our own online research, we estimate the cost of one year's worth of credit monitoring for an individual to cost \$150. Using that figure, three years' worth of credit monitoring would amount to \$450 per person. In our example above, we used an even lower estimate of \$300 per person.

Programs, 17 NO. 5 *Intell. Prop. & Tech. L.J.* 20 (2005). In order to resolve a suit brought by the Federal Trade Commission, Choice Point agreed to pay \$10 million in civil penalties and another \$5 million in consumer redress. *See* Warren Agin, *Information Security Law*, 26-3 *ABIJ* 54 (April 2007). Other corporate victims of lost or stolen data include Bank of America, which lost the personal information, including names and social security numbers, of approximately 1.2 million federal employees; DSW Shoe Warehouse, a retailer from whom 1.4 million credit card numbers were stolen; and TD Ameritrade, an online brokerage from whom cyber-criminals stole the personal information of approximately 6.3 million customers. These are but a few examples of the many companies that have experienced significant cyber-risk losses in recent years, whether as a result of theft, accident or their own inadvertence or carelessness.

In another noteworthy matter, Fidelity Federal Bank and Trust (“Fidelity”), a West Palm Beach-based bank, settled a class action lawsuit brought by Florida motorists for an estimated \$50 million, including \$10 million in attorneys’ fees to plaintiffs’ counsel. *See* Jeff Ostrowski, *Tens of Thousands of South Florida Drivers to Get \$160 Checks*, *Palm Beach Post* (December 8, 2006). Fidelity allegedly violated federal anti-stalking legislation, which prohibits companies from buying driver records from state governments, when it purchased the records of approximately 565,000 Florida drivers between 2000 and 2003. *Id.* Fidelity reportedly purchased the information for a penny a name from the Florida Department of Highway Safety and Motor Vehicles, and then used the information to mail out brochures advertising its auto loans. *Id.* The plaintiffs involved in the settlement will each receive \$160. *Id.*

It is evident that the recent advances in technology that have driven the growth of e-commerce have also resulted in unforeseen potential liabilities for businesses. Whether through a lack of foresight, a failure to understand and appreciate the potential perils of new technology or, perhaps, an underestimation of the determination of cyber-criminals to gain access to confidential data, many companies have left themselves uninsured against potential losses arising out of the storage of electronic data. Recognizing and acknowledging the presence of those perils will enable a company to protect itself from losses that may arise out of new technologies.

Insurance is one of the most common devices utilized by businesses to safeguard against catastrophic losses. Traditional insurance policies, however, were not designed to protect against the cyber-risks. As a result, many businesses that have, until now, relied solely or primarily on their comprehensive general liability (“CGL”) policies will likely find themselves unprotected against the risks presented by many new technologies.

This paper will present an overview of certain technological advancements and the risks those advancements pose to businesses. We will also address the insurance coverage issues presented by so-called “cyber-risks” under a CGL policy and why businesses facing cyber-risk liabilities may find themselves without insurance protection. Moreover, we will discuss cyber-risks from an underwriting and risk management perspective, providing an overview of what may be done to protect against such risks.

While the trials and tribulations of companies such as TJX and other businesses that have fallen victim to lost or stolen data are noteworthy and have been the subject of significant media attention, they do not represent the only examples of cyber-risks that may befall a business in the digital age. For example, a business might inadvertently

post copyrighted content on its website, leading to claims of copyright infringement, or host a chatroom or bulletin board on which, if not monitored vigilantly, potentially defamatory or private information may be posted, resulting in claims for defamation or invasion of privacy. In another scenario, an internet worm or computer virus might shutdown or paralyze a company's computer network or website, resulting in lost sales or a shut-down in operations until the problem is corrected. Moreover, a ripple effect may be felt by other businesses that, for example, may rely on another company's network or website for the placement of orders.

For purposes of the present discussion, we will focus on two potential cyber-risks faced by any business that has a computer network or engages in e-commerce over the internet: lost or stolen data.

B. *Storage of consumer data as a "cyber-risk"*

For years, large corporations have collected and stored a wide range of consumer information to assist in marketing and sales efforts. Quite often, that information consists of sensitive personal and financial data of consumers, including credit card numbers and, in the United States, social security numbers and other personal, identifying information. New technologies have dramatically decreased the cost of collecting consumer data and storing it electronically. Because of the decreased cost of storage, and the miniaturization of memory devices and their ease of use, many smaller businesses are now utilizing the same tools as some larger companies in the gathering and storing of consumer data.

As demonstrated by the incident involving TJX, the costs of data security breaches are potentially astronomical, and may include the costs of: government and regulatory investigations, government fines or penalties, court orders, injunctive relief,

consumer class action litigation, vendor litigation, damaged business reputation, customer loss, loss of goodwill, shareholder suits and internal investigation costs. *See* John F. Delaney, *Privacy, Data Security, and Outsourcing the Regulatory Framework*, 8444 PLI/Pat 611, 617 (October 24, 2005). A company may even find itself the victim of data extortion after a network security breach, wherein a cyber-criminal holds the stolen data for “ransom.” It is also not uncommon for businesses to incur costs on expensive public relations campaigns after a breach in order to improve its public image.

What’s more, in light of recently enacted data notification laws, businesses may be required, at their own cost, to notify each and every individual whose personal information may have been lost or stolen. Accordingly, a business can also expect losses and claims that include the cost of notifying the public and individual customers that their personal information or credit card numbers have been stolen and even the cost of paying for credit monitoring on behalf of customers in order to safeguard against identity theft.

C. Storage of a company’s own proprietary or essential business information as a “cyber-risk”

In addition to the perils posed by the loss of consumer data and other third-party information, businesses must also act to safeguard their own proprietary business information and other forms of electronic data that are essential to keep their business running smoothly and seamlessly. This can include not only such things as customer lists, project designs and other forms of “intellectual property,” but also the computer programs on which business operations run, including accounting software, inventory-tracking software, and the software and programming required to keep assembly lines functioning and e-commerce websites on-line.

D. Data Notification Laws

A series of high-profile data breaches in the first half of 2005 prompted U.S. lawmakers to introduce more than a half-dozen bills that would require companies to notify consumers affected by security breaches. David Bank, *Breaches of Customers' Data Trigger Lawsuits*, *The Wall Street Journal* (July 21, 2005). "Some of the bills have exceptions for encrypted data, and some require companies to report breaches only when they determine there's significant risk to customers." Grant Gross, *2006 in Congress: 'Full Plate' for Tech, Telecom* (December 27, 2005), available online at <http://www.itnetcentral.com/article.asp?id=15395&leveli=0&info=home>. What some commentators, business leaders and lobbyists have referred to as a "patchwork quilt" of state laws has led to calls for a national data breach law that preempts state laws. Grant Gross, *Data Breach Bills Unlikely to Pass before 2006* (November 11, 2005), available online at http://www.infoworld.com/article/05/11/11/HNdatabreachbill_1.html. Federal legislation dealing with data breach notification has been introduced in both the House of Representatives and in the Senate, and would require businesses and other organizations to disclose data breaches that result in the loss of consumers' personal information. See Brian Krebs, *Data Breaches Spur Congressional Action, Federal Notification Law Would Trump State Measures* (July 18, 2005), available online at <http://www.washingtonpost.com/wpdyn/content/article/2005/07/18/AR2005071800613.html>. The main objectives of the proposed bills are:

1. Greater protection of and control over the use of key personal data such as Social Security numbers and financial account information;
2. Increased penalties for breaches and facilitating identity theft; and

3. A nationwide standard for notifying consumers when their personal information has been breached. *See* Jeanne Sahadi, *Breaches: Federal Law on the Way? Lawmakers have Proposed Several Bills that Seek to Better Protect Personal Data*, (July 7, 2005), available online at http://money.cnn.com/2005/07/06/pf/security_bills/.

While those bills remain pending before Congress, legislation has already been enacted requiring certain business to properly protect consumer/client data. The Federal Financial Modernization Act, commonly know as Gramm-Leach-Bliley Act (“GLBA”), 15 U.S.C. § 6801 *et seq.*, was passed by Congress and signed by President Clinton in November, 1999. The GLBA states, “[i]t is the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those consumers’ non-public information.” 15 U.S.C. § 6801. Section 501(b) of the GLBA mandates that financial institutions develop and implement administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information. Put simply, it requires financial institutions to prevent unauthorized access to non-public, personal information.

The Health Insurance Portability and Accountability Act (“HIPPA”) , 42 U.S.C.. § 1320(d) *et seq.*, and The Sarbanes-Oxley Act of 2002 (“SOX”), 15 U.S.C. § 7201 *et seq.*, are two other federal laws that also mandate that electronically stored consumer/client information be adequately protected.

As mentioned, a number of states (at least 35) have enacted or introduced legislation regarding customer notification of security breaches that result in the

unauthorized release of personal consumer information. California was the first state to enact legislation governing the disclosure and notification of data security breaches to effected consumers. Many states have followed suit, modeling their notification laws after California's. Generally, the legislation requires companies "to notify consumers regarding breach of security in which certain personal information relating to those consumers was, or is reasonably believed to have been, acquired by an unauthorized person." Thomas E. Scanlon, *Overview of Recent State Laws Requiring Notification of Security Breach*, 6 NO. 3 Privacy & Info. L. Rep. 6 (Nov. 2005). Each state's data notification statute, however, is not identical, containing its own nuances.

California's Database Security Breach Notification Act, codified at Cal. Civ. Code § 1798.82 and § 1798.29, and General Security Standard for Businesses, codified at Cal. Civ. Code § 1798.81.5, requires companies and government agencies that store personal information on California residents to implement safety procedures that safeguard data and disclose any breach of security to the individuals affected. Cal. Civ. Code § 1798.82 (a) affects any state agency, business, or person that conducts business in California and maintains computerized data that includes personal information. Cal. Civ. Code § 1798.82 (b) states that any breach of the security of the data must be reported in the most expedient manner following the discovery of the breach to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Cal. Civ. Code § 1798.82 (e) defines personal information as an individual's last name and first name or initial, in combination with a Social Security number; driver's license or California ID Card number; or account, debit card or credit card number, in combination with any security code, access code or

password that would permit access to the account. Cal. Civ. Code § 1798.82 (g) provides that:

“[N]otice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency’s Web site page, if the agency maintains one.

(C) Notification to major statewide media.

Failure to promptly notify the information owner or licensee of the data makes the organization liable for civil damages. “The law allows any customer who is injured by a violation of [Cal. Civ. Code § 1798.82] to institute a civil action to recover damages.” Francoise Gilbert, *Information Privacy and Security in California*, 1 NO. ABA SciTech Law. 8 (Fall, 2004). Thus, a company that fails to comply with the notification provisions of Cal. Civ. Code § 1798.82 may face legal action from consumers and, also, from the California Attorney General.

The General Security Standard for Businesses, Cal. Civ. Code § 1798.81, requires that businesses owning or licensing such personal information about a California resident, when held in unencrypted form, implement and maintain reasonable security procedures and practices to protect the personal information from unauthorized access,

use, modification, destruction, or disclosure. California's Database Security Breach Notification Act and General Security Standard for Businesses should have a significant impact on business practices with respect to the protection of electronic data gathered and stored because of the potential for severe penalties. These penalties can be inflicted through class action lawsuits and other penalties and fines that may be levied against the organization for negligence in exercising an inadequate standard of care in protecting the information. In addition, companies face possible additional costs attributable to security breaches, including damage to image, reputation and brand resulting from public awareness of and perception of security breaches, the cost of notifying data owners and the cost of defending lawsuits brought against the company.

Florida passed H.B. 481, Fla. Stat. Ann. § 817.568 *et seq.*, effective July 1, 2005. Fla. Stat. Ann. § 817.5681(1)(a) provides that “[a] person who conducts business in this state and maintains computerized data in a system that includes personal information provide notice of any breach of the security of the system, following a determination of the breach, to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.” There is a forty-five day grace period for notification after the security breach. Fla. Stat. Ann. § 817.5681(b)1 states that if notification to consumers is not performed within this time period, fines of up to \$1000 per day for up to thirty days can be imposed. Pursuant to Fla. Stat. Ann. § 817.5681(b)1, if the company does not notify the customers of the breach after the subsequent thirty day period, the fines increase to \$50,000 for each thirty day period, up to 180 days. If notification is not made within 225 days, any person required to make notification under Fla. Stat. Ann. § 817.5681(b)2 but fails to do so is

subject to an administrative fine of \$500,000. Pursuant to Fla. Stat. Ann. § 817.5681(10)(b), fines of up to \$50,000 are specified for failure to document the breach, or for failure to keep records of the breach for up to five years.

Most of the state notification laws track the California or Florida notification statutes by generally defining "personal information" as an individual's name, plus any one or more of the following "data elements:" the individual's Social Security number, driver's license or state identification card number, or account number in combination with a password or other access code for the account, when either the name or the data elements are not encrypted. However, some of the state notification laws apply to a broader range of information. Therefore, companies looking to comply with the consumer notification laws on a nationwide basis should consider increasing security measures for all data elements that any of the states include in the definition of "personal information," to the extent they retain such data elements.

II. INSURANCE COVERAGE FOR CYBER-RISKS UNDER A TYPICAL COMPREHENSIVE GENERAL LIABILITY POLICY

A business exposed to cyber-risks, whether through the collection and storage of consumer data or its own business data, or through its maintenance of its own website, chatroom or internet bulletin board, faces significant financial uncertainty if its sole protection against third party liability is the CGL insurance policy, one of the most pervasive types of insurance purchased by businesses. The CGL policy indemnifies the insured for liability to third parties for bodily injury, property damage, personal injury and advertising injury that is unintended from the perspective of the insured. It provides this coverage under two primary coverage parts; Coverage A, which provides cover for

“bodily injury” or “property damage” liability; and Coverage B, which provides coverage for “personal injury” and “advertising injury” liability.

Losses arising from new technologies do not neatly fit, if at all, within the insuring agreements of traditional CGL policies. Under Coverage A, property damage liability is typically defined as “physical injury to tangible property, including all resulting loss of use of that property,” as well as “loss of use of tangible property that is not physically injured.” The question thus arises whether electronic data can be considered “tangible” property. Another question is whether cyber-risk exposures in the nature of intellectual property, defamation and invasion of privacy claims are covered under Coverage B. For example, although an invasion of privacy claim is customarily among the specifically-enumerated “personal injury” offenses under a CGL policy, many policies will require a publication or utterance before granting cover for such a claim. Or, to fall under the “advertising injury” coverage grant of Coverage B, there must be a nexus between the policyholder’s advertising activities and the offending activity.

In short, there are numerous gaps in coverage for cyber-risks under traditional CGL policies. Moreover, revisions to the CGL policy forms, beginning in 2001, have attempted to specifically limit coverage for cyber-risks. One significant change to the standard-form CGL policy, for example, attempts to expressly exclude electronic data from “tangible” property damage coverage.

It is beyond the scope of this paper to address each and every coverage issue raised by the different potential claims that could arise out of cyber-risk claims, including the potential first-party claims of businesses that experience such things as computer

viruses, hacker attacks and internet service provider outages.³ To highlight some issues, we discuss the insurance coverage issues potentially implicated in a claim for property damage under Coverage A arising out of a data breach or loss or a claim for personal or advertising injury liability arising out of internet liability that potentially falls under Coverage B.

A. Data held to be “intangible”

Generally, courts interpreting the pre-2001 CGL language have held that data is not “tangible” property and have denied coverage for claims arising out of damaged or lost data. Most CGL policies provide cover only for tangible property damage and Courts in most jurisdictions have expressly held that a standard CGL policy does not provide coverage for loss of “intangible” property. *See, e.g., Guelich v. American Protection Ins. Co.*, 772 P.2d 536 (Wash. Ct. App. 1989); *Columbia Nat. Ins. v. Pacesetter Homes, Inc.*, 532 N.W.2d 1, 6 (Neb. 1995). Until recently, the prevailing view has been that electronic data is not tangible property damage that is covered under a CGL policy. *See, Lucker Mfg. v. Home Ins. Co.*, 23 F.3d 808, 818 (3d Cir. 1994) (“Tangible property is property that can be felt or touched, or property capable of being possessed or realized.”); Paul M. Yost, et al., *In Search of Coverage in Cyberspace: Why the Commercial General Liability Policy Fails to Insure Lost or Corrupted Data*, 54 SMU L. Rev. 2055, 2066-68 (2001).

In State Auto Prop. and Cas. Ins. Co. v. Midwest Computers & More, 147 F. Supp.2d 1113, 1116 (W.D. Okl. 2001), the United States District Court for the Western

³ Although the terminology varies from policy to policy, first-party coverage provided by most commercial property policies generally requires “physical loss or damage to covered property that results from a covered cause of loss.” *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers’ Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). Accordingly, whether there has been damage to tangible, physical property will also be an issue with respect to first-party property policies.

District of Oklahoma held that electronic data is not tangible property for purposes of insurance coverage. Midwest Computers & More (“Midwest”) was insured under a business owners’ liability policy issued by State Auto Property and Casualty Insurance Company (“State Auto”). *Id.* at 1114. That policy provided coverage for “property damage” to “tangible property,” and defined “property damage” as:

- a. Physical injury to tangible property, including all resulting loss of use of that property; or
- b. Loss of use of tangible property that is not physically injured.

[*Id.*]

In 1999, William C. Spray and Patricia Spray, doing business as Spray Appraisals (“Spray”), purchased a computer from Midwest and hired Midwest to perform certain computer services for the business. *Id.* Spray later alleged that Midwest negligently performed its computer service work, allegedly causing Spray to be deprived of the use of its computers and to lose extensive amounts of appraisal data and other business information which was stored on its computer system. *Id.* at 1114-15. When Midwest sought coverage under its business owners’ liability policy, State Auto filed suit, seeking a declaratory judgment that it had no duty to defend or indemnify Midwest under the policy. *Id.* at 1115.

Both Midwest and State Auto agreed that the relevant issue to be decided was whether the computer data alleged to have been destroyed by Midwest was “tangible property” within the meaning of the business owners’ liability policy. *Id.* The Court, however, determined that this issue alone was not dispositive on the issue of coverage and identified another issue: whether a loss of a computer occurred and, if so, whether the

loss of a computer satisfies the second part of the policy's definition of property damage, namely, loss of use of tangible property that is not physically injured. *Id.*

With respect to the issue of whether the lost data could be considered "tangible" property, the Court stated that the term "tangible" should be given its plain, ordinary and accepted meaning as something "capable of being perceived, especially by the sense of touch . . . capable of being precisely identified or realized by the mind." *Id.* at 1115-16. According to the Court, the ordinary meaning of the term tangible does not fit data stored on a computer disk or tape. *Id.* at 1116. Although the medium that holds the information (*i.e.*, the disk or tape) can be perceived, identified or realized, the information itself cannot be. *Id.* Because data itself cannot be touched, held or sensed by the human mind, the Court held that it cannot be considered tangible property. *Id.*

The Court next turned its attention to the issue of whether the loss of a computer can be considered property damage. Because a computer itself is tangible property, the Court held the "loss of use" of computers as a result of Midwest's alleged negligence to be property damage within the meaning of the policy. *Id.* As discussed in further detail below, however, Midwest was left without coverage after the Court determined that a policy exclusion precluded coverage for the claim at issue. *Id.*

This same reasoning was applied by the United States Court of Appeals for the Fourth Circuit in *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003). Shortly after the internet service provider America Online, Inc. ("AOL") released its Version 5.0 access software in October 1999, it was hit with a number of consumer class action lawsuits in state and federal court in the United States from consumers alleging damage to their computer system and preexisting software. *Id.* at 91. In short,

the consumer complaints alleged that AOL Version 5.0 altered the plaintiffs' existing computer software, disrupted their network connections, caused the loss of stored data and caused their operating systems to crash. *Id.* at 91-92. AOL tendered the defense of the consumer actions to St. Paul Mercury Ins. Co. ("St. Paul"), which denied coverage on the basis that the claims "do not allege damage to 'tangible' property and are not property damage as defined by the St. Paul [commercial general liability] policy." *Id.*

Like the Court in *Midwest Computers*, the Fourth Circuit in *America Online* applied to the term "tangible" its ordinary meaning of something that is capable of being touched and perceived in the physical sense. *Id.* at 94. Thus, it distinguished tangible computer hardware from intangible data, information and instructions. *Id.* at 95. The Court drew a distinction between "data or instructions and the physical machines that give them meaning." *Id.* It reasoned that:

Instructions to the computer and the data and information processed by it are abstract ideas in the minds of the programmer and the user. The switches and the magnetic disks are media, as would be paper and pencil. Loss of software or damage to software thus is not damage to hardware, but to the idea, its logic, and its consistency with other ideas and logic. Of course, without any code and instructions, the hardware consists simply of millions of electronic switches, circuits and drives that can be turned on or off but that cannot function as a computer. To a user, such a computer would be "dead." But regardless of whether the software is rendered unusable, the hardware remains available for instructions and recording.

[*Id.* at 95-96.]

The Court also analogized hardware to a tangible pad lock and data to the intangible combination to the lock: although the lock may be unusable without the combination, it is not physically damaged. *Id.* at 96.

It was in this light that the Court examined the allegations made by the consumer plaintiffs and determined that “[e]ven though a few . . . complaints [were] vague enough to suppose initially that the plaintiffs complain of damage to physical property, a closer look . . . reveals that the plaintiffs actually complain of damage to software.” *Id.* at 97. Accordingly, it determined that the software problems did not amount to physical damage to tangible property for purposes of CGL coverage. *Id.* at 97-98.

Having determined that consumer claims did not allege physical injury to tangible property, the Court shifted its attention to AOL’s contention that the consumers’ loss of use of their computers constituted covered property damage. *Id.* at 98. The District Court sitting below had agreed with AOL that the consumers’ loss of use of hardware was property damage within the meaning of the policy, but denied coverage based on the policy’s “impaired property” exclusion. *Id.* As discussed in further detail below, the Fourth Circuit, on appeal, upheld the application of the impaired property exclusion as a bar to coverage, but declined to address the issue of whether the consumers’ alleged loss of use of their computers was a tangible loss. *Id.* at 99.

B. Data held to be “tangible”

A minority of courts have granted coverage, usually where the loss of use of hardware on account of damaged or lost data was an element of the claim for loss of electronic data. However, recent decisions suggest that Courts may be moving away from traditional distinctions between tangible and intangible property, at least with respect to electronic data.

In a controversial decision, the United States District Court for the District of Arizona, in *American Guarantee & Liability Ins. Co. v. Ingram Micro, Inc.*, 2000 U.S.

Dist. LEXIS 7299 (D.Ariz. 2000), held that loss of data and programming information constituted physical loss or damage under a first-party property policy.

Ingram Micro, Inc. (“Ingram”), a wholesale distributor of microcomputer products, was insured by American Guarantee & Liability Insurance Company (“American Guarantee”) under a property damage policy that provided coverage against certain business interruption and service interruption losses. *Id.* at *1-*2. Ingram utilized a world-wide computer network known as the Impulse System (“Impulse”) to track its customers, products and daily transactions. *Id.* at *2-*3. All of Ingram’s orders, whether received electronically or through telephone sales representatives, were processed through Impulse, making its entire business operation dependant upon the proper functioning of Impulse. *Id.* at *3.

On the morning of December 22, 1998, Ingram’s data center suffered a power outage that shut down all electronic equipment at the center, including computers and telephones. *Id.* at *3-*4. Although power was restored within a half-hour of the failure, Ingram’s three mainframe computers lost all programming information that had been stored in their random access memory. *Id.* at *4. That lost programming information had to be manually re-loaded by Ingram employees. *Id.* It was not until approximately eight hours after the shut down that Ingram was able to restore Impulse to full power. *Id.* at *5. Ingram then sought coverage under its property damage policy with American Guarantee for the substantial business and service interruptions it suffered as a result of the power outage.

American Guarantee denied coverage and filed a declaratory judgment action against Ingram, claiming that its computer system had not been “physically damaged.” It argued that:

[T]he computer system and [other hardware] were not “physically damaged” because their capability to perform their intended functions remained intact. The power outage did not adversely affect the equipment’s inherent ability to accept and process data and configuration systems when they were subsequently reentered into the computer system.

[*Id.* at *5-*6.]

Ingram, in response, argued that the fact that the mainframe computers and other hardware retained their ability to accept restored information and eventually operate as before did not mean that they did not undergo “physical damage.” *Id.* at *6. Ingram offered a broader definition of the term “physical damage,” contending that it includes loss of use and functionality. *Id.*

The Court sided with Ingram’s broader definition of property damage “[a]t a time when computer technology dominates our professional as well a personal lives.” *Id.* It held that ““physical damage”” is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.” *Id.* As support for its holding, the Court looked to federal and state “cyber-crime” laws that defined “damage” as impairment, alteration, degradation or destruction of a computer system or network. *Id.* at *6-*7. It found these definitions to be relevant, despite the fact that they did not appear in insurance coverage cases, on the basis that:

Lawmakers around the country have determined that when a computer’s data is unavailable, there is damage; when a computer’s services are interrupted, there is damage; and when a computer’s software or network is altered, there is

damage. Restricting the Policy's language to that proposed by [American Guarantee] would be archaic.

[*Id.* at *7.]

Accordingly, the Court held that Ingram Impulse system had been “physically damaged” for eight hours and that Ingram, not American Guarantee, was entitled to summary judgment on the issue of coverage. *Id.* at *8-*9.

The Court's decision in *Ingram Micro* was widely criticized, as the Court violated well-established principles governing insurance contract interpretation -- namely, that the ordinary meanings of words in a contract control. Instead of giving effect to the word “physical,” as it is ordinarily used, the Court simply read it out of the contract in order to reach its desired conclusion.

Although *Ingram Micro* involved the meaning of the term “physical” under a first-party property policy, it is nevertheless relevant to coverage under a CGL policy because the meaning of “physical” and “tangible” are closely related. *Ingram Micro* is noteworthy in that if a Court can conclude that loss of data amounts to a physical loss, it can just as easily conclude that data is “tangible” property under a CGL policy.

That is precisely what happened in *Computer Corner, Inc. v. Fireman's Fund Ins. Co.*, 46 P.3d 1264 (N.M. Ct. App.), *cert. den.*, 47 P.3d 447 (N.M. 2002). Computer Corner, Inc. (“Computer Corner”) engaged in the sale and service of personal computers. Fireman's Fund Insurance Company (“Fireman's”) issued a CGL policy to Computer Corner. *Id.* at 1265. A customer brought his computer to Computer Corner for repair, and expressly informed the Computer Corner technician that various important files were on the computer and were not backed up. *Id.* at 1265-66. Nevertheless, the technician reformatted the hard drive without first backing-up its data. *Id.* As a result, the data was

irretrievably lost. *Id.* The customer thereafter filed suit against Computer Corner seeking damages for the cost of reconstructing its files. *Id.* Firemen's agreed to defend Computer Corner under a reservation of rights, but denied any duty to indemnify it. *Id.* at 1266.

The Court in *Computer Corner* did not specifically address the issue of whether the lost data constituted "tangible" property, as the District Court sitting below had concluded that "computer data is tangible property" and this ruling was not challenged by the parties. *Id.* Although the District Court's decision is not published, the Court of Appeals quoted the lower court as stating that the computer data at issue "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed." *Id.* As discussed in further detail below, the Court's decision addressed the applicability of several policy exclusions that the lower court had held precluded coverage. *Id.* at 1268-70. Accordingly, it reversed the ruling of the lower court and held that Firemen's had a duty to indemnify Computer Corner under its CGL policy. *Id.* at 1270.

Recently, a New York state court, in a decision that may have implications on questions of insurance coverage, abandoned the traditional tangible/intangible property distinction when it comes to electronic data. *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 285-86 (N.Y. 2007), involved the question of whether a claim for conversion of electronic data is cognizable under New York law. Louis E. Thyroff ("Thyroff"), an insurance agent for Nationwide Mutual Insurance Company ("Nationwide"), was discharged from his job and denied access to "his customer information and other personal information that was stored on the [company] computers."

Id. at 285. See also Nick Ackerman, *Protecting Data with an Ancient Remedy*, The National Law Journal (October 3, 2007). Thyroff sued Nationwide in federal court for, among other things, “the conversion of his business and personal information.” *Thyroff*, 8 N.Y.3d at 285. The federal district court dismissed his claim on the grounds that conversion does not apply to intangible computer data. On appeal, the Second Circuit Court of Appeals determined that New York state law was not clear as to whether a claim for conversion could be based on computer data and certified to the New York Court of Appeals, the state’s highest court, the question of whether a claim for conversion of electronic data is cognizable under New York law. *Id.* at 285-86.

The New York Court of Appeals answered this question in the affirmative, holding that electronic records maintained on a computer are “subject to a claim of conversion in New York.” *Id.* at 293. In so doing, the Court reviewed the evolution of the tort of conversion in accordance “with emerging societal values.” *Id.* at 286-88. It looked as far back as the Norman conquest of England in 1066, when a “rightful ownership of property” was usually determined by a physical altercation between victim and thief. *Id.* The medieval practices were eventually replaced by legal actions for trespass, trover and, ultimately, conversion, with New York later modifying conversion’s strict requirement for tangible property to provide that “an intangible property right can be united with a tangible object for conversion purposes.” *Id.* at 286-89. This modification of the law of conversion became known as the “merger doctrine,” and required a connection between the intangible property and a tangible object. Thus, for example, intangible shares of stock in a company could be considered the proper subject of a claim for conversion because they were represented by tangible stock certificates.

Thyroff represents an abandoning of the merger doctrine. The Court recognized that a “document stored on a computer hard drive has the same value as a paper document kept in a file cabinet.” *Id.* at 292. The Court also relied on the pervasive use of computer data as a replacement for paper documents and determined that “the tort of conversion must keep pace with the contemporary realities of widespread computer use.” *Id.* at 292.

Thyroff has implications that potentially reach beyond claims for conversion and may represent how U.S. courts view electronic data in future cases. While there are still jurisdictions that cling to the merger doctrine,⁴ *Thyroff* appears to be the trend. For example, in *Kremen v. Cohen*, 337 F.3d 1024, 1031 (9th Cir. 2003), the Ninth Circuit Court of Appeals held that California law does not follow the strict merger doctrine when it upheld a conversion claim for the intangible property right in an internet domain name. Courts in other conversion cases have likewise assumed that computer data is subject to a claim for conversion without reference to the tangible/intangible property distinction. *See, generally*, Ackerman, Nick, *Protecting Data with an Ancient Remedy*, *The National Law Journal* (October 3, 2007).

Given the growth of and increasing importance of electronic data as an asset in and of itself, *Thyroff* is a well-reasoned opinion that may be looked to as precedent in a challenge to an insurer’s denial of coverage for a cyber-risk loss of data claim under a CGL policy.

⁴ *See, e.g., Slim CD Inc. v. Hartland Payment Sys., Inc.*, 2007 U.S. Dist. LEXIS 62536 at *12 (D.N.J. Aug. 24, 2007); *Northeast Coating Techs. Inc. v. Vacuum Metallurgical Co. Ltd.*, 684 A.2d 1322, 1324 (Maine 1996).

C. Potentially Applicable Exclusions under Coverage A

Even where loss of data may be considered damage to tangible property or loss of use of tangible property that is not physically injured, coverage may ultimately be precluded by one or more applicable policy exclusions, including, but not limited to:

Business Risk Exclusions

In *Midwest Computers, supra.*, 147 F.Supp.2d at 1113, the Court held that the customer's "loss of use" of its computers as a result Midwest's allegedly negligent computer services to be "property damage," but in the end declared that the "business risk" exclusion of the business owners' liability policy at issue barred coverage. *Id.* at 1116-18. That exclusion precluded coverage for property damage to "that particular part of any property that must be restored, repaired or replaced because 'your work' was incorrectly performed on it." *Id.* at 1116. Further, the Court held that the Products-Completed Operations exception to the exclusion did not apply because the underlying Complaint alleged that the loss had occurred before Midwest had completed its work. *Id.* at 1117.

On the contrary, the Court in *Computer Corner, supra.*, 46 P.3d at 1264, held that the business risk exclusions in the policy at issue did not preclude coverage, where the Court had already held lost computer data to be "tangible" property. One of the business risk exclusions at issue in *Computer Corner* provided that the insurance did not apply to "property damage to your product arising out of it or any part of it." *Id.* at 1268. The other business risk exclusion provided that the insurance did not apply to "property damage to your work arising out of it or any part of it and included in the products-completed operations hazard." *Id.* The Court's ultimate conclusion with respect to both

the “your property” and “your work” business risk exclusions was that the property that was lost -- the customer’s computer files -- clearly existed prior to and apart from any service or parts provided by Computer Corner in repairing the computer and was thus not Computer Corner’s “product” or “work.” *Id.* Moreover, it also found nothing in the applicable exclusions or definitions that would have suggested to a reasonable insured in Computer Corner’s position that “property damage to your product” or “property damage to your work” includes damage to a customer’s pre-existing electronic data. *Id.* Accordingly, the Court held that the business risk exclusions did not apply.

Impaired Property Exclusion

Another example of a policy exclusion that may act to bar coverage in a cyber-risk case is the Court’s application of the “impaired property” exclusion in *America Online, supra.*, 347 F.3d at 98. There, the Court held that the loss of computer data and damage to software was not damage to tangible property and, because it also found that the impaired property exclusion applied, it did not specifically answer the question of whether the losses could be considered “loss of use” property damage. The relevant portions of the impaired property exclusion at issue in *America Online* provided:

We won’t cover property damage to impaired property, or to property which isn’t physically damaged, that results from:

. . . your faulty or dangerous products or completed work;

* * *

Impaired property means tangible property, other than your products or completed work, that can be restored by nothing more than:

. . . an adjustment, repair, replacement, or removal of your products or completed work which forms a part of it . . .

[*Id.*]

AOL argued that the impaired property exclusion could not be applied because the underlying consumer complaints “allege[d] physical damage to and loss of use of computers that could not be fixed simply by repairing, removing, or replacing AOL Version 5.0, thus taking the claims outside the definition of impaired property.” *Id.* According to the Court, however, that argument failed to address what it termed the “relevant portion” of the impaired property exclusion which, in edited form, provided that: “We won’t cover property damage [including loss of use of tangible property] . . . to property which isn’t physically damaged, that results from . . . your faulty . . . products.” *Id.* The Court believed that the “straightforward meaning” of the impaired property exclusion barred coverage for loss of use of tangible property of others that is not physically damaged by the insured’s defective product and placed a limitation on the coverage of consequential damages, restricting coverage to loss of use other persons’ properties that are physically damaged. *Id.* The Court further explained that without the limitation of coverage to property that is physically damaged, the insurer’s risk would have been much greater and it would have been asked to defend a wide range of claims that did not involve physical damage to tangible property. *Id.* According to the Court, the limitation imposed by the impaired property exclusion was designed specifically to deny coverage for this broader risk. *Id.* And because there was no specific allegation that the physical or tangible components of any computer were damaged (only that software caused damage to other software), the Court concluded that the impaired property exclusion applied. *Id.* at 99-100.

On the other hand, the Court in *Computer Corner, supra.*, 46 P.3d at 1264, concluded that a similar “impaired property” exclusion did not apply to preclude coverage. The particular exclusion at issue in *Computer Corner* provided that the insurance did not apply to:

Property damage to impaired property or property damage that has not been physically injured arising out of:

(1) A defect, deficiency, inadequacy or dangerous condition in your product or your work; or

(2) A delay or failure by you or anyone acting on your behalf to perform a contract or agreement in accordance with its terms.

This exclusion does not apply to the loss of use of other property arising out of sudden and accidental physical injury to your product or your work after it has been put to its intended use.

[*Id.* at 1268-69.]

In short, the Court found the impaired property exclusion to be “complicated” by the incorporation of multiple terms (“property damage,” “impaired property,” “your product,” “your work”) defined elsewhere in the policy. *Id.* at 1269. It ultimately concluded that the exclusion was “unintelligible from the standpoint of a hypothetical reasonable insured operating a computer repair service.” *Id.* at 1270. It therefore held the exclusion to be too vague and indefinite to be enforceable. *Id.*

Intentional Acts Exclusion

CGL policies typically contain an “intentional acts exclusion” that bars coverage for bodily injury or property damage “expected or intended from the standpoint of the insured.” The applicability of an intentional acts exclusion was also among the issues examined by the Court in *Computer Corner, supra.*, 46 P.3d at 1264, where the insured’s

computer technician reformatted a customer's hard drive without first backing-up the data. To make matters worse, the customer had also informed another of the insured's technicians that the hard-drive's data was important and had not been previously backed-up. In the end, the Court refused to apply the intentional acts exclusion, finding that the failure of one technician to report to another technician the fact that the customer expressly instructed that the files be backed-up was "the result of mis-communication, mistake or carelessness, rather than a conscious decision to cause harm to the [the insured's] property." *Id.* at 1267. Moreover, the Court found that there was no evidence that the technician who reformatted the hard drive understood that it contained the only copy of certain files and that by reformatting it he would be contributing to the permanent loss of data. *Id.* at 1269. Accordingly, the Court held that the loss of data was neither "expected nor intended" from the perspective of the insured and did not act to exclude coverage. *Id.*

Electronic Data Exclusion

The current ISO CGL form policy provides that the insurance provided under Coverage A does not apply to:

Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.

As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.

[CGL Policy Form CG 00 01 12 04, ISO Properties, Inc., 2003.]

This amendment to the CGL policy takes aim at those judicial decisions that have found damage to data to be damage to tangible property and should make clear to policyholders that on a going-forward basis insurers do not intend to provide cover for losses of electronically stored data under the traditional CGL policy.

D. Personal and Advertising Injury Coverage for Cyber-Risk Claims

We also examine the potential for coverage of certain cyber-risk offenses under Coverage B, as insureds may also seek coverage under traditional CGL policies for cyber-risk claims involving defamation, invasion of privacy and intellectual property exposures, such as copyright or trademark infringement, to name a few. These will most typically arise in connection with internet websites, chatrooms and bulletin boards, including websites on which a business sells or advertises its products or services.

The term “personal and advertising injury” is typically defined to mean:

[I]njury, including consequential bodily injury, arising out of one or more of the following offenses:

* * *

- d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person’s or organization’s goods, products or services;
- e. Oral or written publication, in any manner, of material that violates a person’s right of privacy;
- f. The use of another’s advertising idea in your “advertisement”; or
- g. Infringing upon another’s copyright, trade dress or slogan in your “advertisement”.

The term “advertisement” is typically defined to mean:

[A] notice that is broadcast or published to the general public or specific market segments about your goods, products or services for the purpose of attracting customers or supporters.

[*Id.*]

Further, in light of the internet and e-commerce boom of the last decade, this definition has been modified to include that, for purposes of the definition of “advertisement”:

- a. Notices that are published include material placed on the Internet or on similar electronic means of communication; and
- b. Regarding web-sites, only that part of a web-site that is about your goods, products or services for the purposes of attracting customers or supporters is considered an advertisement.

[*Id.*]

This language addresses the realization of the ISO drafters that internet advertising and marketing is now an important way that merchants disseminate information about their goods and services, but the language in subsection (b) appears to narrow the coverage businesses receive with respect to information on their website. *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers’ Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). For example, information about a competitor’s products or other unrelated products produced by other manufacturers, links to other websites and banner advertising by other businesses that appear on the insured’s website all seem to fall outside of this definition of “advertisement.” *Id.*

Accordingly, in order for a copyright or trademark infringement claim arising out of internet activities to be considered a “personal or advertising injury,” it must arise out of the insured’s advertising activities, as defined in the policy.

Likewise, for a cyber-related defamation or invasion of privacy claim to be covered as a “personal or advertising injury,” the defamatory material must have been “published.” In other words, a publication or utterance of the defamatory or private material is required before coverage can be found.

As for potentially-applicable exclusions, the CGL policy has long excluded coverage for insureds who are in the business of advertising, broadcasting, publishing or telecasting. *Id.* Recent revisions to the ISO CGL form have placed certain Internet-based businesses squarely within this exclusion, as follows:

This insurance does not apply to:

j. Insureds In Media And Internet Type Businesses

“Personal and advertising injury” committed by an insured whose business is:

* * *

(2) Designing or determining content of websites for others; or

(3) An Internet search, access, content or service provider.

* * *

For the purposes of this exclusion, the placing of frames, borders or links, or advertising, for you or others anywhere on the Internet, is not by itself, considered the business of advertising, broadcasting, publishing or telecasting.

[*Id.*]

Coverage is also now typically excluded, under the Electronic Chatrooms Or Bulletin Boards exclusion, for:

“Personal and advertising injury” arising out of an electronic chatroom or bulletin board the insured hosts, owns, or over which the insured exercises control.

[*Id.*]

Thus, for example, if an insured defames a business competitor on an industry-specific chatroom, a claim arising out of that event should be excluded from coverage pursuant to this exclusion.

Finally, we also note that the so-called “intellectual property exclusion” may act as another bar to coverage under Coverage B. That exclusion provides that the insurance does not apply to:

“Personal and advertising injury” arising out of the infringement of copyright, patent, trademark, trade secret or other intellectual property rights.

However, this exclusion does not apply to infringement, in your “advertisement,” of copyright, trade dress or slogan.

[*Id.*]

This broadly-phrased exclusion does not effectively leave much intellectual property coverage available to insureds. *See* Robert H. Jerry, *Cybercoverage for Cyber-Risks, An Overview of Insurers’ Responses to the Perils of E-Commerce*, 8 Conn. Ins. L. J. 7 (2001/2002). It specifically excludes patent, trademark and trade secret infringement claims from coverage as “personal and advertising injury” and also excludes “other intellectual property rights.” *Id.* In fact, the exclusion is so broad that it requires an exception to the exclusion to grant back the limited intellectual property coverage

afforded under Coverage B to “copyright, trade dress or slogan” in the insured’s “advertisement.” *Id.*

E. Potential Coverage under Directors’ and Officers’ and Errors and Omissions Policies

We briefly discuss two additional types of insurance coverage that may be implicated in a cyber-risk claim: Directors’ and Officers’ (“D&O”) insurance and Errors and Omissions (“E&O”) insurance. D&O insurance indemnifies individual directors and officers sued in connection with the discharge of their corporate duties. *Id.* E&O policies offer defense against and indemnification for claims arising from “negligence, omissions, mistakes, and errors by the insured in the course of providing professional services.” *Id.*

Typically, D&O policies are comprised of two types of coverage: (1) coverage for defense costs and other related expenses and (2) indemnification of covered individuals for third-party liabilities. *Id.* Designed to cover acts such as negligence and errors in judgment, D&O policies may, for example, provide protection against shareholder derivative actions predicated on allegations of breach of fiduciary duty based on the purported failure to implement measures to prevent such cyber-risks as computer hacker attacks. *Id.*

E&O policies, traditionally tailored and marketed to professionals such as lawyers and physicians, have now also been specifically geared toward computer consultants, software and hardware providers and e-commerce and technology experts. *Id.* We discuss in Section III below other new forms of technology oriented insurance created to specifically provide coverage for the new forms of cyber-risks not covered under traditional CGL and other types of policies.

As discussed above, the standard form CGL policy has been amended to ensure that there is no ambiguity on the issue of whether insurers now consider lost electronic data to be property damage and whether such policies provide cover for such damage. However, as a result of the growth of e-commerce and the storage of electronic data (and the new types of claims they have wrought), insurers have begun to address the need in the insurance marketplace for cyber-risk policies that are specifically designed for cyber-related losses and liability. *Insuring Cyberspace: Why Traditional Insurance Policies are not Enough: The Nature of Potential E-Commerce Losses & Liabilities*, 3 Vand. J. Ent. L. & Prac. 84, 89 (Winter 2001). Insurance companies now offer a wide-range of cyber-risk insurance to cover losses due to cyber activities. *Id.* For example, some now offer coverage for security breaches by providing coverage for computer equipment, electronic data and storage-related risks. *Id.* The new cyber-risk policies have removed the issue of whether lost electronic data is “tangible” property by explicitly providing coverage for computer equipment, hard drives, electronic data processing, software exposure and system break downs. *Id.*

III. THE DEVELOPMENT OF CYBER-RISK INSURANCE AND CYBER-RISK MANAGEMENT

A. *Cyber-risk insurance*

“Cyber-risk insurance” is really an umbrella term that can encompass many different types of coverages, ranging from data theft and computer malfunction to external hacking, internal sabotage and theft, web-content liability and copyright infringement, to name a few. The cyber-risk insurance market was virtually non-existent ten years ago. By 2005, the cyber-risk insurance market was estimated to amount to between \$250 million to \$300 million in written premium. Toby L. Merrill, *Cyber*

liability market is older, wiser, smarter and still growing, available online at <http://www.insurancejournal.com/magazines/west/2007/01/29/features/76734.htm>. By 2006, it had burgeoned into a \$500 million market that continues to expand. *Id.*

Network Liability and Privacy Liability policies are two types of cyber-risk policies that can be viewed as “gap filler” policies intended to fill gaps in an overall insurance program for non-physical/non-tangible loss and liabilities. A Network Liability policy would include coverage for restoration costs, namely, the cost to replace, restore or recreate the insured’s lost data or customized program lost as a result of a hacker or system failure. Public relations expenses might also be covered. This would encompass the costs of retaining a public relations consultant to help restore or protect the insured’s reputation in response to adverse media coverage as a result of a cyber-attack or system failure resulting in lost or stolen data. Coverage might be also had for investigative expenses necessary to respond to a cyber loss so that damage may be minimized or mitigated, and future damage prevented. Investigative expenses might also include the cost of gathering evidence demonstrating wrongdoing. A Network Liability policy might also include cover for extortion threats, in the form of reimbursement of costs incurred in responding to a threat to introduce an unauthorized code into the insured’s computer system or to divulge private data without authorization.

A Privacy Liability policy, which insures against liability arising from the unauthorized disclosure or loss of private information, might provide enhanced coverage for an insured’s failure to protect confidential information. Such a policy might also provide coverage for credit monitoring and credit remediation for the individuals whose confidential information had been compromised; vicarious liability of the insured when

control of confidential information is outsourced to an outside vendor; public relations expenses; regulatory defense costs; government imposed fines and penalties; and the cost of notifying individuals that their personal data had been lost or stolen.

Some other types of typical cyber-risk insurance coverage products on the market today include: General Internet Crime Liability, which addresses first and third party risks associated with e-commerce, the internet, networks and informational assets; Property Liability, which protects against damage to hard assets caused via the internet, machinery taken down or equipment programmed to operate erratically (but typically does not acknowledge “data” as property); and Media Liability Coverage, which protects against claims arising out of the gathering and communication of information, providing coverage against defamation and invasion of privacy claims as well as copyright and trademark infringement. Denis Drouin, *Cyber Risk Insurance: A Discourse and Preparatory Guide*, GIAC Security Essentials Certification, Practical Assignment Version 1.4a, option 1 (February 9, 2004). A cyber-risk policy might also provide Business Income Loss coverage, which would encompass earnings loss and extra expenses loss as a result of non-physical events such as a hacker attack or a computer virus. Coverage for Business Income Loss might also include loss of revenues from websites or as a result of supply chain failures caused by viruses, hackers or employees maliciously causing a system to crash. *Id.*

Chubb, for example, is one insurer that now offers a variety of cyber-risk insurance products, including a policy marketed as “CyberSecurity by Chubb for Financial Institutions.” *See* <http://www.chubb.com/business/csi/chubb822.html>. According to Chubb, that policy is intended specifically for financial institutions and is

designed to address their most vulnerable e-commerce exposures in one straightforward policy. The policy consists of six insuring clauses, described by Chubb as follows:

- **E-Theft:** Designed to protect against losses resulting from: (1) the transfer, payment or delivery of funds or other property due to a cyber attack; (2) the misappropriation, copying or duplication of confidential customer information or records by hacker or employees who breach network security; and (3) the physical loss or damage of stolen electronic media.
- **Denial or Impairment of E-Service:** Designed to protect the financial institution when its system is subject to cyber-attack or fraudulently accessed, *regardless of whether there has been direct physical loss or damage to tangible property*. This includes system slowdowns or shutdowns caused by cyber attacks, such as worming or spamming.
- **E-Communication:** Applies when an electronic communication is sent from one financial institution to another to initiate, authorize or acknowledge a monetary transaction, and the communication was either not sent by the insured institution or was fraudulently modified during the electronic transmission.
- **E-Vandalism:** Helps the financial institution pay for the direct cost of restoring the integrity of its site in the aftermath of hackers' vandalism of any data, instructions or communications within the system.
- **E-Threat:** Protects against threats made against the institution's system that could result in taking the system off-line or a breach in network security (*e.g.*, the release of confidential customer information). Reimburses the institution for expenses incurred to mitigate loss in the event of an alleged threat (provided the threat is technologically credible), rather than wait for the perpetrator to act on such a threat and risk any downtime. Also pays for fees and expenses of any public relations consultant if the firm has been the target of such a threat.
- **E-Signature:** Protects the institution from direct loss resulting from accepting a customer's electronic signature on loan agreements secured by real property, such as a

mortgage, and then discovering that the signature is fraudulent.

[*Id.*]

The CyberSecurity by Chubb for Financial Institutions policy is but one example of the many types of new insurance products offering coverage for cyber-risks, which, like all insurance products, can be tailored for specific industries and threats.

B. *Risk management guidelines*

Ideally, all businesses would conduct a comprehensive privacy and security audit and promptly implement all recommendations in a timely manner to avoid falling victim to one of the many “cyber-risks” that can victimize a business in today’s electronic world. If a business does not have the resources to conduct its own audit, it should hire an outside company to perform a security assessment. Likewise, as part of its underwriting of a cyber-risk policy, an insurer should require that a privacy and security audit of the applicant be performed.

It is beyond the scope of this discussion to offer a comprehensive risk management guideline for managing cyber-risks. However, it is needless to say that any security audit or assessment and any risk management procedures that are put in place carefully examine both a company’s network security and the physical security of its computer hardware. There are a myriad of questions that can be asked in regard to both of these areas. As to network security, some questions that arise are: whether the business has “firewalls” in place to prevent unauthorized access to internally protected networks from external sources; whether authentication vehicles are used to allow connections from remote users into internal networks; how often are firewalls and anti-virus safeguards updated; and whether the business has a dedicated response team and

continuity plan in the event of a security breach. As to physical security, some pertinent questions include: whether a full inventory of all computer-related equipment has been conducted; whether critical computer servers are maintained in a secure fashion; who has access to servers and what access controls are in place; and how sensitive materials and data are safeguarded and disposed of. *See, generally, Denis Drouin, Cyber Risk Insurance: A Discourse and Preparatory Guide, GIAC Security Essentials Certification, Practical Assignment Version 1.4a, option 1 (February 9, 2004).*

Other questions and specific areas of inquiry would depend on the type of business and the size of the business. For example, if a business conducts credit card transactions over the internet the manner in which sensitive consumer data is collected and stored would have to be thoroughly examined. Also, if a business maintains a website, pertinent questions include whether it owns the intellectual property rights to the content on the website and whether it has any established procedures in place for removing infringing or offensive material from its website. How a particular business's revenues would be affected if a security breach occurred is also a question that might be asked from a risk management perspective. *Id.*

Underwriters will, of course, have their own set of questions and issues to address in evaluating a new risk. AON has produced a document setting forth some of the factors examined by underwriters in the context of cyber-risk insurance, specifically, Network Liability coverage. These include:

- **Financial Stability and Lack of Losses:** Some industries are more prone to cyber-risk incidents than others. An insurer must price risk accordingly.

Key Documentation: financial statements and loss runs.

- **Sales Practices and Contract Procedures:** With respect to those businesses engaged in e-commerce, an underwriter will want to examine sales practices to verify mutual expectations of the applicant business and its customers. Limitation of liability clauses, exculpation of warranty provisions and consistent contract review procedures are critical.

Key Documentation: standard contracts and guidelines to amend standard clauses.

- **Dispute Procedures:** How does the business avoid litigation?

Key Documentation: complaint and dispute guidelines.

- **Formal Management Responsibility and Standards:** Companies must successfully demonstrate that the responsibility to maintain a secure network is a responsibility entrusted to a senior individual within the organization, such as a Chief Security Officer, Chief Technology Officer or Chief Operating Officer (or a systems administrator for a smaller company). Network security policies and procedures should be published and communicated to all staff. Network assessment and testing should be conducted according to industry standards.

Key Documentation: written network security policies and procedures, security audit schedules and security audit reports.

- **Physical Network Security Safeguard Controls:** The business needs to demonstrate that its physical environment is “robust” enough to keep cyber-criminals at bay. Along with basic devices such as magnetic access cards for employees and closed circuit television, data centers and server rooms should be accessible only by the IT staff. Staff should know who to call in the event of suspicious activity.

Key Documentation: physical security policies and guidelines, lists of perimeter and internal security elements in place.

- **Logical Network Security Controls:** At a minimum, network security controls should include filters and

firewalls to keep intruders from accessing the network from the Internet or other private networks; antivirus software to keep viruses, worms and other malicious code at bay; and intrusion detection software to identify potential network trespassers. In the event that medical, financial or other non-public personally-identifiable information (*e.g.*, social security numbers) is transmitted over the Internet or stored as electronic data, sufficient encryption standards should be enforced.

Key Documentation: network architecture diagrams, firewall and intrusion detection software make and model information, antivirus vendor information, and a copy of procedures and policies in place to ensure that new equipment is properly configured before it is connected to the network.

- **Change Management Controls:** Policies and procedures must be in place to ensure that network access rights for ex-employees (and sub-contractors) who have been terminated or who have resigned are revoked, and that facility access cards are revoked during exit interviews.

Key Documentation: written employee resignation and termination guidelines in network security planning document.

- **Internet Content Controls:** Businesses must be able to document written controls over the posting of information on websites. These include, but are not limited to, legal reviews to ensure that any third party content posted has gone through a formal clearing process and proper management of chat rooms, discussion boards and other interactive areas of company sites.

Key Documentation: written rules, including legal reviews, regarding the posting of content on company sites.

- **Disaster Recovery and Business Continuity Planning:** This is a critical component of any Network Liability risk submission, particularly where contractually guaranteed network availability is offered to customers or network interruption coverage is required by the applicant. Companies with large networks should be prepared to demonstrate that formal disaster recovery and business continuity plans are in place not only to protect critical

data, but also to ensure that network availability is maintained in the event of a natural disaster or hacker attack. Elements include, but are not limited to, data backup and recovery testing and redundant applications and connections.

Key Documentation: Disaster recovery and business continuity planning reports and outlines.

[AON, *Network Risk Insurance: A Layman's Overview* (October 2004).]

Finally, we note that it is also critical that all businesses ensure that they are aware of and in compliance with all applicable data notification laws, some of which are described above.

All of this brings us back to TJX. Investigators in the TJX case believe that the data breach began when hackers pointed a telescope-shaped antenna at a Marshall's store in St. Paul, Minnesota, and used a laptop computer to decode data streaming through the air between hand-held price-checking devices, cash registers and the store's computers. That helped them hack into TJX's central database to repeatedly purloin customer information and credit card numbers. A post-breach audit has revealed that TJX was slower than many merchants to make a change to a more complex and wireless encryption system called Wi-Fi Protected Access, or WPA. The audit also found that TJX failed to install firewalls and data encryption on many of its computers using the wireless network, and did not properly install another layer of network security software it thought it had purchased. *See Joseph Pereira, Breaking the Code: How Credit Card Data Went Out Wireless Door, The Wall Street Journal* (May 4, 2007).

Proper and thorough underwriting and the implementation of a “cyber-risk” risk management program can help prevent businesses from becoming the next TJX and, at the same time, will help to cut insurers’ losses on cyber-risk claims.

IV. CONCLUSION

Advanced and accessible computer technologies have provided businesses both large and small with new opportunities in the world of e-commerce. At the same time, those new opportunities have come with risks heretofore unseen by businesses and insurers alike. The cyber-risks represented by lost or stolen data and the other perils of the cyber-age do not neatly fit under the coverage of traditional insurance policies such as CGL policies, with their requirement of “tangible” property loss and other policy language affording coverage for the “brick and mortar” business losses of years past. Moreover, potential coverage exclusions abound under both Coverage A and Coverage B. At the same time as it has revised the standard ISO form CGL policy to further limit coverage for cyber-risks, the insurance industry has introduced new cyber-risk-specific products that move beyond the traditional areas of coverage and recognize that, to today’s businesses, data is just as “tangible” as any other valuable property. Both insurers and insureds need to be aware of the new risks and must plan accordingly through implementation of cyber-risk specific underwriting and risk management guidelines and the purchase of cyber-risk insurance.



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

*A Change in Climate:
The Chilling Effect of Global Warming*

Kevin T. Coughlin, Esq.
Kevin MacGillivray, Esq.
Amanda K. Coats, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

I. INTRODUCTION.....2

II. CLIMATE CHANGE LITIGATION3

III. THE LEGAL THEORIES OF CLIMATE CHANGE LITIGATION4

 A. Suits Against Public Agencies to Compel Regulation of GHG Emissions.....5

 B. Suits Against Private Entities for Injunctive Relief and Monetary Damages..7

IV. MASSACHUSETTS V. EPA9

 A. Summary of Massachusetts v. EPA.....9

 B. The Impact of Massachusetts v. EPA.....11

V. CLIMATE CHANGE LITIGATION AND INSURANCE.....14

 A. Tort Lawsuits, CGL Policies and the Absolute Pollution Exclusion.....14

 B. Directors and Officers Insurance Policies19

VI. CONCLUSION21

COUGHLIN DUFFY LLP

I. INTRODUCTION

In August 2005, Hurricane Katrina ripped through Louisiana and Mississippi leaving behind a wake of destruction that still affects the region. Classified as the costliest natural disaster in United States history, economic damages resulting from Hurricane Katrina are estimated to exceed \$10 billion (US). Not surprisingly, environmentalists and scientists immediately attributed Hurricane Katrina's severity to one cause – global warming.

Hurricane Katrina is but one example cited by environmentalists and scientists in support of the devastating effects of global warming. In August 2007, eight straight days of torrential rains in the Midwest of the United States resulted in unprecedented flooding, 18 deaths and in excess of \$115 million (US) in property damage. A prolonged heat wave in the western United States this past summer caused temperatures to soar above 100 degrees Fahrenheit, resulting in devastating droughts, wildfires, freeway closures, property damage, and deaths. Similar destruction has occurred across the globe. The Indian Ocean Tsunami of 2004 resulted in approximately 300,000 deaths and in excess of \$10 billion (US) in damage. In each of these cases, global warming was cited as a contributing factor.

The question remains, however, to what extent will the insurance industry feel the economic heat of “climate change litigation,” tabbed by plaintiffs’ attorneys as the next tobacco litigation? To date, climate change litigation in the United States has been slow to develop. The initial climate change lawsuits were instituted by environmental groups, states and even private citizens against public agencies seeking to secure equitable and legal relief from the effects of climate change in light of legislative inaction. To a lesser extent, climate change lawsuits have been instituted against private entities such as automobile manufacturers, chemical companies and power companies. Inasmuch as the United States is the world’s largest global warming

polluter, legal prognosticators anticipate an increase in climate change lawsuits against industrial companies whose products, facilities and plants emit greenhouse gases (“GHG”). For those who insure this targeted class, it is with bated breath that they await action by the United States’ government and courts as to whether such lawsuits are viable.

The United States Supreme Court’s landmark decision in Massachusetts v. EPA¹ has the potential to drastically alter the course and impact of climate change litigation in the United States. As discussed in greater detail below, the Supreme Court’s decision could open the door to lawsuits against private entities on the theory that they caused global warming through GHG emissions. If that occurs, the insurance industry can anticipate a landslide of claims by the target defendants seeking coverage for their actions that allegedly contribute to global warming.

In this paper, we discuss the development of climate change litigation in the United States. Our discussion includes a breakdown of the reported decisions against both governmental and private entities, as well as a detailed discussion of the Supreme Court’s decision in Massachusetts v. EPA and its potential impact on future climate change litigation. Finally, we discuss the imminent influence of climate change lawsuits on casualty insurers. In particular, we discuss the applicability of pollution exclusions to global warming claims and the implications on directors and officers (“D&O”) insurance policies stemming from the failure to disclose and/or reduce GHG emissions.

II. CLIMATE CHANGE LITIGATION

Climate change is “any significant change in measures of climate (such as temperature, precipitation, or wind) lasting for an extended period (decades or longer).”² The term climate change is used interchangeably with global warming to refer to the rise in the Earth’s atmospheric temperature as a result of an increase in heat-trapping greenhouse gases (e.g. carbon

dioxide, methane, and nitrous oxide).³ From 1990 to 2005, GHG emissions rose 16%.⁴ Carbon dioxide alone, the leading GHG emission, rose 20%.⁵ The effects of climate change range from catastrophic weather events to “sea level rise, shrinking glaciers, changes in the range and distribution of plants and animals, trees blooming earlier, lengthening of growing seasons, ice on rivers and lakes freezing later and breaking up earlier, and thawing of permafrost.”⁶ Climate change even affects societies’ environments and lifestyles.⁷

The pervasive effects of climate change prompted queries into the appropriate responsive measures. In the past, environmental crises were addressed by the legislature through initiatives such as the Clean Air Act (“CAA”). However, climate change has gone unchecked by federal, state and local legislatures. For example, the United States Environmental Protection Agency (“EPA”) was petitioned by several states and environmental groups on October 20, 1999, to exercise its authority under the CAA to regulate the GHG emissions of new motor vehicles.⁸ The EPA’s denial of the petition on September 8, 2003, prompted the lawsuit and subsequent Supreme Court decision in Massachusetts v. EPA.⁹ Despite these recent events, Congress and federal agencies remain hesitant to directly address the problem.¹⁰ As a result, “[l]awsuits are proliferating [and likely will continue] in the absence of federal regulatory action.”¹¹

III. THE LEGAL THEORIES OF CLIMATE CHANGE LITIGATION

The current view of climate change litigation, particularly in the wake of Massachusetts v. EPA, is that it has the potential to be the next series of tobacco cases. To consider the potential of this litigation, we must review prior climate change litigation – the theories used and the success rates. For ease of discussion, this section is broken down into two parts:

- (A) suits against public agencies to compel regulation of GHG emissions; and
- (B) suits against private entities for injunctive relief and monetary damages.

COUGHLIN DUFFY LLP

The following is a non-exhaustive list of climate change lawsuits filed to date. Analysis of the legal theories employed and impediments faced by litigants will foster a better understanding of the potentials and the pitfalls of this new litigation.

A. Suits Against Public Agencies to Compel Regulation of GHG Emissions

Litigation to enforce regulation of global warming was conceived in the early 1990s. Though the science underlying climate change litigation is ever-evolving, the nature of climate change litigation has changed little since then. Major obstacles faced by litigants remain, including standing and justiciability challenges.

In Los Angeles v. Nat'l Highway Traffic Safety Admin.,¹² petitioners, including cities, states, and environmental groups, challenged a federal agency's decision not to prepare an environmental impact statement addressing the global warming impact of relaxing the Corporate Average Fuel Economy ("CAFÉ") standards for automobile model years in the late 1980s.¹³ The court found petitioners had standing to sue based upon their obligations under the CAA and the National Environmental Protection Act ("NEPA"). A party has standing to sue if he or she has a personal stake in the outcome of the litigation in the form of a concrete injury causally connected to the defendant's actions that is capable of redress that does not assert a political question or generalized grievance for which the court lacks jurisdiction to review.¹⁴ In finding that the GHG emissions conferred standing, the majority stated, "the evidence in the record suggests that we cannot afford to ignore even modest contributions to global warming."¹⁵

Conversely, in Foundation on Economic Trends v. Watkins,¹⁶ the court held that environmental organizations did not have standing to assert a claim against several federal agencies that were alleged to have failed to adequately address the effects of federal reactions to global warming as required under the NEPA. The court found plaintiffs' claim for

COUGHLIN DUFFY LLP

“informational injury to be virtually indistinguishable from an ideological interest in the problem of global warming that, without more, is insufficient to confer standing.”¹⁷ Despite these inconsistent rulings on the issue of standing, such lawsuits continued. In fact, climate change lawsuits even flourished due to global environmental initiatives such as the Kyoto Protocol and increased public awareness.

The most common lawsuits filed regarding enforcement of environmental regulations arise out of the provisions of the CAA or CAA-based state emissions standards. For example, in Coke Oven Environmental Task Force v. EPA,¹⁸ various states, major cities, and environmental groups sued the EPA, alleging it failed to establish a new source performance standard as required under the CAA. Similarly, in Central Valley Chrysler-Jeep, Inc. v. Witherspoon,¹⁹ several automobile manufacturers and dealers challenged a California law requiring all motor vehicles sold in the state to meet emission standards for carbon dioxide, methane, nitrous oxide, and hydrofluorocarbons. Both cases were stayed in light of the decision pending in Massachusetts v. EPA which also dealt with the EPA’s authority to regulate global warming pursuant to the provisions of the CAA. As of the date of this paper, Witherspoon is expected to be remanded and Coke Oven is scheduled for rehearing October 2007.²⁰

The provisions of the CAA were also considered in Northwest Environmental Defense Center et al. v. Owens Corning.²¹ Environmental organizations sued Owens Corning for building a facility without a preconstruction permit required under the CAA. Owens Corning moved to dismiss for lack of standing. The Oregon District Court found plaintiffs had standing to sue based on (1) the facility’s contribution to global warming, (2) the facility’s harm to members of plaintiffs’ organizations, and (3) plaintiffs’ sufficiently concrete and particularized injury though it was of “wide public significance.”²² Ultimately, this case settled; Owens

COUGHLIN DUFFY LLP

Corning agreed to concessions including withdrawal of the permit and payment of monies toward environmental projects in Oregon.²³

Finally, the decisions in Border Power Plant Working Group v. Department of Energy²⁴ and Center for Biological Diversity v. Abraham²⁵ signaled a potential turning point on the issue of standing. In Border Power Plant, environmentalists alleged that the Department of Energy's ("DOE") failure to appreciate the environmental impact of electrical lines installed across the US-Mexican border violated federal regulations, including the NEPA. Plaintiffs' geographic proximity to the proposed electric lines and the interest in protecting the public health conferred standing. Specifically, the Border Power Plant court, forecasting the holding reached in Massachusetts v. EPA in relation to the EPA's regulation duties pursuant to the CAA, held that the DOE's environmental analysis was inadequate because it failed to address the emissions impact of carbon dioxide emissions.²⁶

The California courts went even further in Abraham. Environmental organizations alleged that various federal agencies failed to enforce the provisions of the Energy Policy Act of 1992 related to alternative fuel vehicles. Plaintiffs' concerns about global warming were deemed "too general, too unsubstantiated, too unlikely to be caused by defendants' conduct, and/or too unlikely to be redressed by the relief sought to confer standing."²⁷ Nonetheless, the court found plaintiffs had standing to sue because pollution would be lessened if the agencies fulfilled their obligations under the Act. Hence, the courts opened the door to expand the standing requirements and the rationale was adopted by the Supreme Court in Massachusetts v. EPA.

B. Suits Against Private Entities for Injunctive Relief and Monetary Damages

Though less prevalent than cases seeking enforcement of environmental regulations, lawsuits against private entities are acutely significant due to their potential impact on insurers.

COUGHLIN DUFFY LLP

To comprehend the current state of climate change litigation, it is important to understand the courts' position on tort damages pre-Massachusetts v. EPA, and the potential changes flowing from that decision.

In Connecticut v. American Electric Power, Inc.,²⁸ eight states and New York City brought suit pursuant to federal common law public nuisance and sovereign interests against the five largest emitters of carbon dioxide among electricity generators. Each of these electric companies is considered a private entity. The consolidated case alleged that defendants' carbon dioxide emissions contribute to global warming. The Court for the Southern District of New York dismissed the complaint as a non-justiciable political question, finding that resolution of the issues requires "identification and balancing of economic, environmental, foreign policy, and national security interests."²⁹ The decision has been appealed.³⁰

In Barasich v. Columbia Gulf Transmission Co.,³¹ Louisiana residents sued various privately-held companies in the wake of Hurricane Katrina for tort damages caused by erosion to Louisiana's coastal wetlands. The United States District Court for the Eastern District of Louisiana found that plaintiffs asserted a justiciable question, noting that the plaintiffs in Barasich, unlike the plaintiffs in Amer. Elec. Power, Inc.,³² sought damages rather than injunctive relief that did not require extensive policy determinations rising to the level of a non-justiciable political question.³³ The case was nevertheless dismissed for failure to state a cause of action under Louisiana law.

The foregoing cases illustrate the issues that have to date plagued climate change litigation, including questions of standing, the authority to regulate GHG emissions, and the tort rights arising from global warming. But as illustrated in the next section, the pivotal case of

Massachusetts v. EPA (partially) resolved these obstacles and has the potential to greatly impact climate change litigation in the United States.

IV. MASSACHUSETTS V. EPA

A. Summary of Massachusetts v. EPA

The catalyst for this watershed decision was a rule-making petition that was filed “[o]n October 20, 1999, [by] a group of 19 private organizations . . . asking EPA to regulate ‘greenhouse gas emissions from new motor vehicles under § 202 of the Clean Air Act.’”³⁴ As background, the CAA was first enacted in 1970 and most recently amended in 1990 in response to the growing problem of air pollution. The CAA, in pertinent part, sets forth the EPA’s authority to act with regard to motor vehicle air pollution, stating:

The Administrator shall by regulation prescribe (and from time to time revise) in accordance with the provisions of this section, standards applicable to the emission of any air pollutant from any class or classes of new motor vehicles or new motor vehicle engines, which in his judgment cause, or contribute to, air pollution which may reasonably be anticipated to endanger public health or welfare.³⁵

Further, the CAA defines an “air pollutant” as “any air pollution agent or combination of such agents, including any physical, chemical, biological, radioactive . . . substance or matter which is emitted into or otherwise enters the ambient air.”³⁶ These provisions of the CAA were relied upon to petition the EPA as to GHG emissions. After much delay, the EPA ultimately denied the petition, claiming that it lacked the authority under the CAA to regulate climate change and, even if it had the authority, the exercise of same was improper.³⁷ As a result, the petitioners filed suit in the United States District Court for the District of Columbia. The questions ultimately certified to the United States Supreme Court were “whether EPA has the statutory authority to regulate greenhouse gas emissions from new motor vehicles; and if so, whether its stated reasons for refusing to do so are consistent with the statute.”³⁸

COUGHLIN DUFFY LLP

The threshold issue that the Supreme Court considered was whether the petitioners had standing to sue. As outlined above, for a party to have standing to sue, he or she must have a personal stake in the outcome of the litigation in the form of a concrete injury causally connected to the defendant's actions that is capable of redress.³⁹ Also, “[w]hen a litigant is vested with a procedural right, that litigant has standing if there is some possibility that the requested relief will prompt the injury-causing party to reconsider the decision that allegedly harmed the litigant.”⁴⁰

Pursuant to the aforementioned standard, the Supreme Court concluded that Massachusetts had standing to sue. First, petitioners have a right to challenge the EPA's actions pursuant to the CAA. Second, the Court found petitioners had standing to sue because of “Massachusetts’ stake in protecting its quasi-sovereign interests”⁴¹ and its “particularized injury [of coastal erosion] in its capacity as a landowner.”⁴² Of particular note is the Court's finding that even though climate change risks are widely shared and regulation may only slow GHG emissions, Massachusetts still had a particularized injury capable of redress.⁴³ In sum, the Court determined that the alleged injuries of coastal erosion suffered by petitioners were concrete and sufficiently causally related to motor vehicle GHG emissions such that it was appropriate for petitioners to challenge the EPA's actions pursuant to the CAA.

The next question before the Court was whether the EPA has authority to regulate GHG emissions pursuant to the CAA. Based upon the definition of “air pollutant” in the CAA,⁴⁴ the Court concluded that it does. Though the Legislature may not have appreciated the possibility of global warming when the CAA was originally enacted in 1970, the broad definition of airborne compounds includes carbon dioxide.⁴⁵ There was no basis to construe the term in another way. Therefore, the Court held that the “EPA has the statutory authority to regulate the emission of such gases from new motor vehicles.”⁴⁶ As a result, the Court remanded the matter for the EPA

to reconsider the petition and base its reasoning for denying or approving the petition on the language of the CAA.⁴⁷

B. The Impact of Massachusetts v. EPA

The impact of Massachusetts v. EPA on climate change litigation cannot be overstated. As demonstrated in Part III of this paper, prior litigation was oftentimes marred by problems of standing and allegations that federal agencies lacked authority to act, but the Supreme Court dealt with these problems in Massachusetts v. EPA. Hence, analysis of this watershed decision is important to deduce what problems were resolved and what questions remain unanswered.

First, the Supreme Court determined that the EPA had authority to control GHG emissions pursuant to the CAA. This precedential decision can therefore be extended to reach similar conclusions with regard to the CAA in other contexts and other statutory frameworks that were enacted to combat particular environmental ills. For example, in Green Mt. Chrysler Plymouth Dodge Jeep v. Dalmasse,⁴⁸ automobile manufacturers and local dealers challenged Vermont's adoption of California's GHG automobile emission regulations as preempted or violative of federal regulations including the CAA. The court found standing to sue based upon plaintiffs' allegations of "[p]robable economic injury resulting from governmental action that alters competitive conditions."⁴⁹

Importantly, after determining that plaintiffs' had standing to sue, the United States District Court of the District of Vermont rendered one of the first post-Massachusetts v. EPA decisions. The court analyzed the Massachusetts v. EPA ruling and held that the CAA-derived state regulations of Vermont, imitating California's laws,⁵⁰ were neither preempted by, nor impermissible under federal law.⁵¹ As a result, there is a reasonable basis for the proliferation of

COUGHLIN DUFFY LLP

climate change lawsuits against federal, state and local agencies to compel regulation of GHG emissions.

Second, the Supreme Court resolved the standing issue in relation to climate change litigation asserted against public agencies. Prior courts under similar circumstances determined that litigants lacked standing because they asserted only generalized grievances.⁵² In response, the Court cautioned that just because “climate-change risks are ‘widely shared’ does not minimize” standing⁵³ and reduction in emissions to slow global warming provides a sufficient impetus to warrant action.⁵⁴ This conclusion was reached despite the fact that there was no absolute causal connection, the possibility of other contributing factors, and the reality that regulation of motor vehicle emissions would not reverse global warming.⁵⁵ Thus, it appears that the Court may have lowered the standing requirement for climate change litigants.⁵⁶

On the other hand, the Court’s standing conclusion created a “special status” for state sovereigns that may have limited applicability.⁵⁷ In fact, a major question remains unresolved – can private litigants sue in tort for damages premised on global warming and GHG emissions? In the wake of Massachusetts v. EPA, it was universally believed that “[t]he decision is likely to embolden climate change litigants.”⁵⁸ Nevertheless, the few decisions applying Massachusetts v. EPA suggest that the courts may be disinclined to extend “standing” to private tort litigants.

In California v. GMC,⁵⁹ the California court expressly denied the right to seek tort damages for global warming. This suit was filed on behalf of the people of California against the six major automobile manufacturers, alleging that under federal and state common law the defendants created a public nuisance. Upon review after the decision in Massachusetts v. EPA, the California court held that plaintiffs’ claims presented non-justiciable issues.⁶⁰ The California court found that the Supreme Court’s decision emphasized the importance of initial policy

COUGHLIN DUFFY LLP

determinations that have not been made by the Legislature in relation to tort claims.⁶¹ Specifically, the California court held that “[w]hile the Supreme Court did not expressly address the issue of justiciability [in Massachusetts v. EPA], it certainly did not sanction the justiciability of the interstate global warming damages tort claim now before this Court.”⁶² The decision may be appealed.⁶³

In the well publicized case of Comer v. Nationwide Mut. Ins. Co.,⁶⁴ Louisiana property owners sought damages from their insurance companies for failing to reimburse plaintiffs for property damage caused by Hurricane Katrina. The suit also included allegations against three privately-held chemical companies for damages sustained during the hurricane that were allegedly partially a result of GHG emissions. The United States District Court for the Southern District of Mississippi required the individual plaintiffs to file separate actions against their insurers because of the particular facts relevant to each claim. The court further noted the difficulty of proving causality with regard to the global warming claims, and decided these claims also had to be filed separate from the insurance claims. Significantly, after the Supreme Court’s decision in Massachusetts v. EPA, the United States District Court for the Southern District of Mississippi dismissed plaintiffs’ claims for lack of standing and plaintiffs’ assertion of non-justiciable claims pursuant to the political question doctrine.⁶⁵ Like California v. GMC, the decision may be appealed.⁶⁶

In light of these recent turn of events, it will be important to see how the courts continue to proceed in this landscape. Although the initial reaction of the courts appears to be rejection of tort lawsuits premised on global warming, it would be unwise to presume that States, public interest groups, private entities, citizens, and the plaintiffs’ bar will be deterred from instituting future tort lawsuits. In fact, law firms in the United States and internationally have already

begun to form climate change teams and have commenced marketing that practice area. It can be expected that plaintiffs' attorneys will continue to file these lawsuits to stretch the bounds of climate change litigation.

V. CLIMATE CHANGE LITIGATION AND INSURANCE

As with other mass tort litigation, climate change litigation against private entities will necessarily have an impact on the insurance industry. Insurers will undoubtedly be asked to provide coverage to GHG polluters for claims asserting liability for their contribution to global warming and the purported damages arising therefrom. As noted by one commentator, insurers can no longer treat "global climate change as a peripheral concern."⁶⁷ In fact, as the industry braces for the impact of climate change litigation, it is important to understand the crisis and anticipate the areas of greatest potential exposure to coverage. Although it is far from certain what legal theories and causes of action will be advanced against alleged GHG polluters, it is anticipated that two types of cases will emerge: (1) public nuisance lawsuits; and (2) shareholder lawsuits against directors and officers. The question presented is whether commercial general liability ("CGL") insurance policies and D&O insurance policies provide coverage for such claims. Of course, the answer to that question may rest in part on whether the pollution exclusions incorporated in such policies will be interpreted by courts to exclude coverage for claims premised on GHG emissions.

A. Tort Lawsuits, CGL Policies and the Absolute Pollution Exclusion

Although only a few tort lawsuits have been filed against companies alleged to be responsible for GHG emissions, the claims asserted in those lawsuits are instructive on the types of claims expected in future climate change lawsuits. For example, in Comer v. Nationwide Mut. Ins. Co.,⁶⁸ plaintiffs sued three chemical companies and five major oil companies alleging

COUGHLIN DUFFY LLP

they caused damage to plaintiffs' property through their contributions to global warming. In California v. GMC,⁶⁹ the State of California sued various automakers under the legal theory of public nuisance. It was alleged that the defendants created and contributed to global warming by producing vehicles that emit high levels of carbon dioxide, which contributes to global warming. The State of California sought damages to study, plan for, monitor and respond to the impact of global warming, which allegedly reduced the supply of water, increased the risk of flooding, eroded California's coastline, and produced extreme heat events that increased the risk and intensity of wildfires.

Indeed, the erosion of the United States' coastlines due to a rising sea level allegedly caused by global warming could prove to be the biggest climate change exposure to GHG polluters and their insurers. The EPA has estimated that a one meter rise in the sea level could result in costs to the United States between \$270 billion and \$450 billion (US). It is not unrealistic to believe that coastline States will institute climate change lawsuits against GHG polluters seeking damages to rebuild, restore, protect and monitor their coastlines. As noted above, California has already sought such relief from various automakers in California v. GMC.

Under the traditional CGL policy, both of the aforementioned lawsuits would arguably trigger coverage since an element of the claims includes "property damage" allegedly caused by the defendants' activities that purportedly contributed to global warming. While it can be anticipated that tort lawsuits premised on global warming will include a component of damages for "property damage," it is also possible that tort lawsuits will include damages for "bodily injury" suffered by victims of catastrophic weather events linked to global warming or outbreaks of infectious diseases purportedly caused by global warming conditions. As with any claim tendered to an insurer, each lawsuit and the allegations asserted therein must be assessed on a

COUGHLIN DUFFY LLP

case-by-case basis to determine whether coverage is even triggered in the first instance. Such an analysis will not only include whether “bodily injury” and/or “property damage” are alleged, but also whether there was an “occurrence” during the policy period that resulted in “bodily injury” and/or “property damage.”

Presuming that the basic insuring agreement is satisfied by the particular allegations of a tort lawsuit premised on global warming, without doubt insureds and their insurers will once again stand toe-to-toe and debate the meaning and intent of the absolute pollution exclusion utilized in CGL policies. The absolute pollution exclusion, introduced by the insurance industry in 1986, provides that coverage is excluded for:

f. (1) “Bodily injury” or “property damage” arising out of the actual, alleged or threatened discharge, dispersal, seepage, migration, release or escape of pollutants:

(a) At or from premises, site or location which is or was at any time owned or occupied by, or rented or loaned to, any insured;

* * *

(2) Any loss, cost or expense arising out of any:

(a) Request, demand or order that any insured or others test for, monitor, clean up, remove, contain, treat, detoxify or neutralize, or in any way respond to, or assess the effects of pollutants; or

(b) Claim or suit by or on behalf of a governmental authority for damages because of testing for, monitoring, cleaning up, removing, containing, treating, detoxifying or neutralizing, or in any way responding to, or assessing the effects of pollutants.

Pollutants means any solid, liquid, gaseous or thermal irritant or contaminant, including smoke, vapor, soot, fumes, acids, alkalis, chemicals and waste. Waste includes materials to be recycled, reconditioned or reclaimed.

COUGHLIN DUFFY LLP

While some absolute pollution exclusions vary in form and language, the above-quoted language is standard.

Despite the seemingly broad nature of the absolute pollution exclusion, the debate has already begun as to whether it applies to claims arising out of GHG emissions. Prior to the Supreme Court's decision in Massachusetts v. EPA, GHGs were not considered "pollutants" by the EPA. However, now that the Supreme Court has classified GHGs as "pollutants,"⁷⁰ the absolute pollution exclusion will once again be scrutinized as to its meaning and scope. That is, courts will be called upon to determine whether the absolute pollution exclusion can be fairly interpreted to include claims premised on GHG emissions.

Unfortunately, there is no clear answer to this question. While the absolute pollution exclusion is arguably intended to exclude all claims arising out of the release of a pollutant, courts are split as to whether its scope extends beyond the hazards associated with traditional industrial environmental pollution. The highest courts in several states have expressly limited the scope of the absolute pollution exclusion to traditional environmental pollution by industrial polluters.⁷¹ Those courts declined to extend the scope of the absolute pollution exclusion to claims that do not involve traditional industrial environmental pollution. For example, the New Jersey Supreme Court declined to interpret the absolute pollution exclusion to bar coverage to an insured that was sued for personal injuries due to exposure to fumes emitted from the insured's painting, coating and floor sealing work.⁷² Similarly, the California Supreme Court held that the absolute pollution exclusion did not apply to claims arising out of injuries caused by exposure to pesticides.⁷³ On the other hand, some courts have construed the absolute pollution exclusion to unambiguously encompass any claim that results from the release of pollutants.⁷⁴

COUGHLIN DUFFY LLP

Undoubtedly, insurers will have a persuasive argument that GHG emissions are “traditional industrial environmental pollution” since the Supreme Court classified GHGs as a “pollutant,” the emission of GHGs has a harmful effect on the environment, and GHG emissions occur in the industrial setting. Moreover, the broad language of the absolute pollution exclusion includes the “release” or “escape” of pollutants. Insureds will likely counter that argument by taking the position that the intent of the exclusion could not include GHG emissions since it was drafted prior to the Supreme Court’s decision in Massachusetts v. EPA. In this regard, insureds will almost certainly argue that it was not within their reasonable expectations that the absolute pollution exclusion would apply to tort lawsuits premised on GHG emissions and global warming. At least one prominent policyholder’s law firm suggested that insureds will also cite to the following facts in support of such an argument: (1) GHG emissions arise from their normal business operations (burning of fossil fuels) and not from the intentional pollution of the environment, as was the case in the past environmental pollution lawsuits; (2) Congress has never regulated GHG emissions; and (3) the EPA has traditionally stated that GHGs do not qualify as pollutants. Moreover, insureds will likely assert that the absolute pollution exclusion was drafted and incorporated in CGL policies in response to traditional industrial environmental pollution claims involving hazardous waste triggering the remedies afforded under the Comprehensive Environmental Response, Compensation & Liability Act (“CERCLA”), and not in contemplation of claims premised on GHG emissions and global warming.

It can therefore be expected that insurers and insureds will once again be at odds with respect to the applicability of the absolute pollution exclusion should climate change lawsuits against private companies proliferate. As was the case with respect to past environmental pollution coverage cases, the ultimate outcome of the applicability of the absolute pollution

exclusion may be dependent on the particular jurisdiction and its historical interpretation of the absolute pollution exclusion.

While the absolute pollution exclusion may prove to be the critical dispute between insurers and insureds with respect to climate change lawsuits, other coverage defenses may also be available to insurers. Such defenses could include the “known loss doctrine” and the applicability of the expected and intended exclusion. With respect to the “known loss doctrine,” insurers may have an argument that their insureds who contribute to GHG emissions have been aware of GHGs’ adverse effect on the environment and have already been placed on notice of claims emanating from their activities. Similarly, insurers may be able to advance the argument that their insureds were aware of the harmful effects of GHG emissions and nevertheless continued with their activities that contributed to global warming. Finally, it can be anticipated that trigger of coverage issues will also arise in the context of climate change lawsuits. For example, with respect to a claim for damages for coastline erosion, insureds would likely argue that a continuous trigger applies to implicate multiple policy years due to the progressive and indivisible nature of the erosion of the coastline.

In summary, should the courts or United States government open the doors for tort lawsuits premised on GHG emissions and global warming, CGL insurers will likely be called upon to defend and indemnify their insureds who have contributed to global warming. Given the nature of such lawsuits, it can be reasonably anticipated that CGL insurers and their insureds will be at odds as whether such claims are covered under a CGL policy.

B. Directors and Officers Insurance Policies

A second type of insurance policy that will be vulnerable to claims stemming from GHG emissions and global warming is the D&O liability policy.⁷⁵ D&O policies are meant to insulate

COUGHLIN DUFFY LLP

directors and officers from lawsuits filed against them regarding actions taken in their professional capacities. These policies generally also contain broad provisions excluding coverage for pollution.⁷⁶ However, the Supreme Court's conclusion that GHG emissions are "air pollutants" under the CAA is likely to encourage shareholders and private litigants to increase the pressure on companies regarding their contribution and response to global warming.⁷⁷

The potential liabilities are two-fold. First, claims may be filed alleging directors and officers breached the fiduciary duties owed to the corporation and the shareholders. The alleged breach may relate to a failure to avoid legal and/or regulatory liability.⁷⁸ As proposed by one practitioner, potential allegations include violating regulations in "their plant operations or manufacturing processes, declining to invest more in research and development to curb greenhouse gases in order to maximize short-term profits from increased sales of their products, and unnecessarily protracting litigation."⁷⁹

Second, claims may allege that directors and officers failed to satisfy disclosure obligations. Pursuant to Item 101 of the Securities Exchange Commission Regulation S-K, "publicly traded companies must disclose current and anticipated material effects from compliance with environmental regulations."⁸⁰ Further, Item 303 requires disclosure of "any known trends or uncertainties that could impact business operations."⁸¹ These disclosure obligations stimulate shareholders to pose questions to a company as to how it "recognizes, analyzes and discloses environmental or climate risk."⁸² For example, 2006 saw the filing of nearly two dozen shareholder resolutions with U.S. companies regarding GHG emissions.⁸³ Without a doubt, the change in the regulatory environment in light of the decision in Massachusetts v. EPA that GHG emissions are "air pollutants"⁸⁴ will make these disclosures more difficult to satisfy and shareholders' questions harder to answer.

COUGHLIN DUFFY LLP

One common reaction to global warming is policy initiatives. Amid the increased concern over global warming generally and the looming liability for directors and officers specifically, companies have implemented plans to reduce GHG emissions.⁸⁵ Though these initiatives are not enough to reverse global warming, many believe that proactive efforts will, at minimum, lessen potential liability and coverage exposure.⁸⁶ As this new horizon comes into focus, insurance companies must begin to appreciate the significance of climate change. Additionally, insurers must anticipate how courts will interpret the provisions of D&O policies and how certain provisions can be improved to insulate against prospective exposures.

VI. CONCLUSION

The debate over global warming – its causes and its consequences – will always exist. The burning questions for insurers are the implications of global warming and the litigation stemming therefrom. Many insurance industry experts believe that it is time for insurance companies to respond to the uncertainties about policy interpretation, shareholder concerns, and SEC disclosure issues related to global warming. For example, it has been suggested that underwriters ask their prospective insureds questions such as:

Does your company allocate responsibility for the management of climate-related risks? Are there independent board members tasked with addressing climate-related issues? What progress, if any, has your company made in quantifying, disclosing and/or reporting its emissions profile and planning for future regulatory scenarios?⁸⁷

Though modifications to policies may be interpreted as an admission that prior policies failed to adequately address this risk, the cost of not responding to the acknowledged risk is perceived as a far greater threat and exposure. Without proper precautions, insurers could be faced with the devastation wreaked upon the insurance industry by other mass tort litigation. The time has come to understand global warming and to what extent its cause and effects are insured.

COUGHLIN DUFFY LLP

-
- 1 127 S. Ct. 1438 (2007).
- 2 U.S. E.P.A., “Climate Change: Basic Information”, at <http://www.epa.gov/climatechange/basicinfo.html> (last visited Sept. 26, 2007).
- 3 Id.; Robert Percival, et al., Environmental Regulation: Law, Science, and Policy, pp. 1122-23 (3rd Ed. 2000).
- 4 U.S. E.P.A., “U.S. Inventory of Greenhouse Gas Emissions and Sinks: 1990-2005: Fast Facts”, USEPA #430-R-07-002, at 1 (Apr 2007), at <http://www.epa.gov/climatechange/emissions/usinventoryreport.html> (last visited Sept. 26, 2007).
- 5 See U.S. E.P.A., “Climate Change: Health and Environmental Effects”, at <http://www.epa.gov/climatechange/effects/index.html> (last visited Sept. 26, 2007).
- 6 “Climate Change: Basic Information”, supra note 2.
- 7 See Id. See e.g. Tenth Session of the Conference of Parties to the United Nations Framework Convention on Climate Change (Dec. 2004), at <http://unfccc.int/meetings/cop10/items/2944.php> (last visited Sept. 27, 2007), for a discussion of the affect on the Inuit environment and the strategies formulated in response to what is alleged to be a violation of their human rights.
- 8 Massachusetts, 127 S. Ct. at 1449. In the rule-making petition, the petitioners alleged that GHG emissions had significantly increased climate change and an important contributor to the acceleration was human activity. Id. (citation omitted).
- 9 Id. at 1450 (citing 68 Fed. Reg. 52922).
- 10 Jonathan H. Adler, “Hot Times in the High Court: Ruling could drive climate-change policy for years to come”, National Review Online (Apr. 3, 2007), at <http://article.nationalreview.com/?q=NmU0ZDBmMmEwZTlkNDBmOTQ3ZTg0YzY5MTM3OTIwNTg> (last visited Sept. 26, 2007).
- 11 Gary Bryner, “The Rapid Evolution of Climate Change Law”, 20 Utah Bar J. 22 (Mar/Apr 2007).
- 12 912 F.2d 478 (D.C. Cir. 1990).
- 13 A similar challenge was filed by various states and environmental groups in Center for Biological Diversity v. Nat’l Highway Trans. Safety Admin., No. 06-71891 (9th Cir. Apr. 6, 2006) regarding CAFÉ standards for trucks.
- 14 Baker v. Carr, 369 U.S. 186, 204 (1962).
- 15 Los Angeles v. Nat’l Highway Traffic Safety Admin., 912 F.2d at 501.
- 16 794 F. Supp. 395 (D.D.C. 1992).
- 17 Watkins, 794 F. Supp. at 399.
- 18 2006 U.S. App. LEXIS 23499 (D.C. Cir. Sept. 13, 2006).
- 19 2006 U.S. Dist. LEXIS 48892 (E.D. Cal. Jul. 7, 2006).
- 20 Environment and Energy Daily, “Climate Change: Domestic Debate – Global Warming Court Cases”, at http://www.eenews.net/special_reports/climate_change_domestic/case_chart/ (last visited Oct. 4, 2007).

21 434 F. Supp. 2d 957 (D.Or. 2006).

22 Northwest Environ. Defense Ctr., 434 F. Supp. 2d at 969.

23 Community Rights Counsel, “Legal Resources: Global Warming Litigation: Clean Air Act Cases”, Apr.
2007, at [http://www.communityrights.org/legalresources/PetitionsForCertiorari/GWC%20and%20](http://www.communityrights.org/legalresources/PetitionsForCertiorari/GWC%20and%20Materials%20CAA.asp)
24 [Materials%20CAA.asp](http://www.communityrights.org/legalresources/PetitionsForCertiorari/GWC%20and%20Materials%20CAA.asp) (last visited Oct. 9, 2007).

24 260 F. Supp. 2d 997 (S.D. Cal. 2003).

25 218 F. Supp. 2d 1143 (N.D. Cal. 2002).

26 Border Power Plant Working Group, 260 F. Supp. 2d at 1028.

27 Abraham, 218 F. Supp. 2d at 1155.

28 406 F. Supp. 2d 265 (S.D.N.Y. 2005).

29 Amer. Electric Power, Inc., 406 F. Supp. 2d at 274.

30 Beveridge & Diamond P.C., “Court Dismisses Global Warming Nuisance Suit on Political Question
Grounds”, dated Sept. 20, 2007, at [http://www.bdlaw.com/assets/attachments/Court_Dismisses_Global_](http://www.bdlaw.com/assets/attachments/Court_Dismisses_Global_Warming_Nuisance_Claim_on_Political_Question_Grounds.pdf)
31 [Warming_Nuisance_Claim_on_Political_Question_Grounds.pdf](http://www.bdlaw.com/assets/attachments/Court_Dismisses_Global_Warming_Nuisance_Claim_on_Political_Question_Grounds.pdf) (last visited Oct. 9, 2007).

31 467 F. Supp. 2d 676 (E.D.La. 2006).

32 406 F. Supp. 2d at 265.

33 Barasich, 467 F. Supp. 2d at 685-86.

34 Massachusetts, 127 S. Ct. at 1449 (citation omitted).

35 42 U.S.C. § 7521(a)(1).

36 42 U.S.C. § 7602(g).

37 Massachusetts, 127 S. Ct. at 1450 (citing 68 Fed. Reg. at 52929-52931).

38 Id. at 1446.

39 Baker, 369 U.S. at 204.

40 Massachusetts, 127 S. Ct. at 1453. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 572 (1992).

41 Id. at 1454-55.

42 Id. at 1456-58.

43 Id.

44 See 42 U.S.C. § 7602(g).

45 Massachusetts, 127 S. Ct. at 1460-62.

46 Id. at 1462.

47 See Massachusetts, 127 S. Ct. at 1463; Massachusetts v. EPA, 2007 U.S. App. LEXIS 22174 (D.D.C. Sept. 14, 2007).

48 2006 U.S. Dist. LEXIS 86805 (D. Vt. Nov. 30, 2006).

49 Dalmasse, 2006 U.S. Dist. LEXIS 86805, at *14.

50 The United States District Court of the District of Vermont referred to related litigation involving similar emissions regulations as originally promulgated by California. See e.g. Central Valley Chrysler-Jeep, Inc. v. Witherspoon, 2007 U.S. Dist. LEXIS 3002 (E.D. Cal. Jan. 16, 2007); Ass'n of Int'l Auto. Manufacturers v. Sullivan, No. 06-CV-69 (D.R.I. Feb. 13, 2006). It is reasonable to anticipate that these other cases will be decided in a similar fashion.

51 Green Mt. Chrysler Plymouth Dodge Jeep v. Crombie, 2007 U.S. Dist. LEXIS 67617 (D. Vt. Sept. 12, 2007) (consolidated action).

52 See e.g. Abraham, 218 F. Supp. 2d at 1143; Utsey v. Coos County, 32 P.3d 933 (Or. Ct. App. 2001); Watkins, 794 F. Supp. at 395.

53 Massachusetts, 127 S. Ct. at 1456.

54 Id. at 1458.

55 See generally Id. at 1438.

56 Adler, supra note 10. See e.g. Nulankeyutmonen Nkihtaqmikon v. Impson, 2007 U.S. App. LEXIS 22053, at *11-18 (1st Cir. Me. Sept. 14, 2007) (found standing to pursue procedural claims under various statutes including the NEPA pursuant to the standing requirement enunciated in Massachusetts v. EPA).

57 Massachusetts, 127 S.Ct. at 1471 (Roberts, dissenting).

58 Allens Arthur Robinson, "Focus: Climate Change Litigation – April 2007", at <http://www.aar.com.au/pubs/ldr/focclapr07.htm> (last visited Sept. 27, 2007).

59 2007 U.S. Dist. LEXIS 68547 (N.D. Cal. Sept. 17, 2007).

60 See Id.

61 Id. at *33-34.

62 Id. at *36.

63 "Climate Change: Domestic Debate – Global Warming Court Cases", supra note 20; "Court Dismisses Global Warming Nuisance Suit on Political Question Grounds", supra note 30.

64 2006 U.S. Dist. LEXIS 33123 (S.D. Miss. Feb. 23, 2006).

65 Order of the United States District Court for the Southern District of Mississippi in Comer v. Nationwide Mut. Ins. Co., dated Aug. 30, 2007, available at http://www.bdlaw.com/assets/attachments/Comer_v_Murphy_Oil_opinion.pdf (last visited Oct. 9, 2007).

66 "Court Dismisses Global Warming Nuisance Suit on Political Question Grounds", supra note 30.

COUGHLIN DUFFY LLP

- 67 Kevin LaCroix, “Climate Change: Directors’ and officers’ risk ahead?”, Insurance Journal, Jun. 4, 2007, available at <http://www.insurancejournal.com/magazines/west/2007/06/04/ideaexchange/81279.htm> (last visited Oct. 4, 2007).
- 68 2006 U.S. Dist. LEXIS 33123.
- 69 2007 U.S. Dist. LEXIS 68547.
- 70 Massachusetts, 127 S. Ct. at 1460-62.
- 71 See e.g., MacKinnon v. Truck Ins. Exchange, 73 P.3d 1205 (Ca. 2003); Am. States Ins. Co. v. Koloms, 687 N.E.2d 72 (Ill. 1997); W. Alliance Ins. Co. v. Gill, 686 N.E.2d 997 (Mass. 1997); Andersen v. Highland House Co., 757 N.E.2d 329 (Ohio 2001); Belt Painting Corp. v. TIG Ins. Co., 795 N.E.2d 15 (N.Y. 2003); Kent Farms v. Zurich Ins. Co., 998 P.2d 292 (Wash. 2000); Nav-Its, Inc. v. Selective Ins. Co., 183 N.J. 110 (2005).
- 72 Nav-Its, Inc., 183 N.J. at 110.
- 73 MacKinnon, 73 P.3d at 1205.
- 74 See e.g., Cont’l Cas. Co. v. Advance Terrazzo & Tile Co., 462 F.3d 1002 (8th Cir. 2006); Nat’l Elec. Mfrs. Ass’n v. Gulf Underwriters Ins. Co., 162 F.3d 821 (4th Cir. 1998); W. Am. Ins. Co. v. Band & Desenberg, 138 F.3d 1428 (11th Cir. 1998); Reliance Ins. Co. v. Moessner, 121 F.3d 895 (3d Cir. 1997).
- 75 Meg Green, “D&O heats up: Directors & Officers writers are paying close attention to the issue of climate change--not just how it could affect Earth, but how it could impact regulations and ultimately lead to future litigation and claims”, Best’s Review, Aug. 1, 2007, available at http://goliath.ecnext.com/coms2/gi_0199-6850255/D-O-heats-up-Directors.html (last visited Oct. 3, 2007).
- 76 Rachel S. Kronowitz, Gilbert Randolph LLP, “United States: Climate Change Exclusion”, May 14, 2007, at <http://www.mondaq.co.uk/article.asp?articleid=48264&searchresults=1> (last visited Oct. 3, 2007).
- 77 See Green, supra note 75; LaCroix, supra note 67.
- 78 Joseph P. Monteleone, Tressler, Soderstrom, Maloney & Priess, LLP, “Global Warming – Will There Be Exposures For Directors and Officers and Will it be Covered?”, Mealey’s Global Warming Litigation Conference, Jun. 6, 2007, at 2, available at <http://www.tsmg.com/pdf/TSMGGlobalWarmingArticle.pdf> (last visited Oct. 9, 2007).
- 79 Id. at 4.
- 80 LaCroix, supra note 67.
- 81 Id.
- 82 Kronowitz, supra note 76.
- 83 Marialuisa S. Gallozzi, “Climate Change: Issues for Policyholders”, The Insurance Coverage Law Bulletin, Vol. 6, No. 4, May 2007, available at <http://www.cov.com/files/Publication/9594b163-512d-4d96-868b-159c28b4eff7/Presentation/PublicationAttachment/d228b807-9251-4dde-86c4-1c46fc74da30/822.pdf> (last visited Oct. 4, 2007).
- 84 Massachusetts, 127 S. Ct. at 1460-62.

⁸⁵ See Green, supra note 75; Adam Aston and Burt Helm, “The Race Against Climate Change: How top companies are reducing emissions of CO2 and other greenhouse gases”, BusinessWeek, Dec. 12, 2005, available at http://www.businessweek.com/magazine/content/05_50/b3963401.htm (last visited Oct. 4, 2007). See e.g. MSNBC, “Power firm agrees to record pollution cleanup: American Electric Power to invest \$4.6 billion to clear Northeast air”, Oct. 9, 2007, available at <http://www.msnbc.msn.com/id/21198255/> (last visited Oct. 9, 2007), for a discussion of American Electric Power’s agreement to pay \$4.6 billion in settlement of a lawsuit alleging violations of the CAA.

⁸⁶ See Green, supra note 75.

⁸⁷ Sally Roberts, “What D&O insurers want to know about risks”, Business Insurance, Aug. 14, 2006, at <http://www.businessinsurance.com/cgi-bin/article.pl?articleId=19442> (last visited Oct. 4, 2007). See Gallozzi, supra note 83.



COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

*Preservation and E-Discovery from a
Litigation and Risk Management
Perspective*

Kevin T. Coughlin, Esq.
Suzanne C. Midlige, Esq.
Robert J. Re, Esq.
Maida Perez, Esq.
Jason Pozner, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 5TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

COUGHLIN DUFFY LLP

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION.....	1
II. WHAT IS ELECTRONICALLY STORED INFORMATION (“ESI”) AND WHERE DO YOU FIND IT?.....	5
A. ESI is Everywhere.....	5
B. Don’t Forget the Metadata.....	8
C. Metadata and the Inadvertent Disclosure of Attorney-Client Communications and/or Confidential or Proprietary Trade Secrets.....	9
III. THE IMPACT OF THE CHANGES TO THE FEDERAL RULES OF CIVIL PROCEDURE ON YOUR ORGANIZATION.....	13
A. The Duty to Preserve Information: Litigation Hold Letters	14
1. What triggers an organization’s obligation to issue a Litigation Hold Letter or Preservation Notice?	16
2. The Essential Elements of an Effective Litigation Hold Letter	20
B. The Scope of the Duty to Preserve: What Data is Potentially Relevant?	23
C. Who Bears the Costs of Producing the ESI?	27
D. Post-Complaint Procedures	29

COUGHLIN DUFFY LLP

IV. **CONSEQUENCES OF NON-COMPLIANCE**.....30

V. **BEST PRACTICES GUIDELINES FOR E-DISCOVERY**

 A. **The Role of the Document Retention and E-mail Retention Policy**35

 B. **E-Discovery Liaison**.....38

VI. **CONCLUSION**40

COUGHLIN DUFFY LLP

I. Introduction

The ubiquitous use of electronic media as a means of communications has had a powerful impact on all aspects of daily life. Corporations and organizations throughout the world have come to rely on electronic media in all facets of their operations. With the globalization of industry, the ability to instantly communicate is a tool that organizations worldwide find indispensable. Notwithstanding its ease of use, electronic communication is not without controversy, particularly where litigation is involved. Indeed, in recent years, we have seen an increasing number of cases wherein courts in the United States have addressed the vast use of electronic data and its impact on litigation in the United States.

United States Courts are continuously carving out and redefining the boundaries of electronic document preservation and production requirements. As a result of the drastic consequences now being sought from and often granted by courts in electronic discovery, organizations and its lawyers must keep a watchful eye on this evolving landscape. In perhaps the most infamous e-discovery sanctions case to date, a Florida jury awarded financier Ronald Perelman \$1.45 billion in damages after the trial judge entered a default judgment against Morgan Stanley as a sanction for various e-discovery missteps.¹ The trial judge found that Morgan Stanley initially certified that all relevant electronic records had been produced, but then repeatedly uncovered new backup tapes months after the discovery deadline had passed. The trial judge ruled that Morgan Stanley had deliberately failed to comply with discovery and instructed the jury to assume that Morgan Stanley had helped to defraud Mr. Perelman. As a result of this instruction, Mr. Perelman had to prove only that he relied on Morgan Stanley's

¹ CPH (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir.Ct., Mar. 1, 2005), rev'd on other grounds, 955 So. 2d 1124 (Fla. Dist. Ct. App., 2007).

COUGHLIN DUFFY LLP

representations to his financial detriment. While the judgment, including the award of punitive damages, was later reversed on grounds unrelated to the electronic discovery issues (which were not discussed by the appellate court), the trial court's rulings and the jury's findings are a cautionary tale of the potential impact of electronic discovery abuses.

The rulings surrounding e-discovery can also be a trap for the unwary or unformed — severe sanctions are not confined to egregious or intentional conduct but can also be assessed for mere ordinary negligence in complying with electronic discovery obligations. The standard for the award of such sanctions was most prominently articulated in the seminal case of Zubulake v. UBS Warburg LLC.² In this employment discrimination case, defendant UBS had taken steps to impose a “litigation hold” to ensure the retention of e-mails and other documents relevant to the litigation. Despite these steps, UBS employees deleted potentially relevant e-mails from their computers. In addition, UBS failed to produce many potentially relevant e-mails that had been retained, and delayed the production of the e-mails that it did produce. The Zubulake court held that the defendant had willfully destroyed potentially relevant e-mails and deserved the sanction of an adverse spoliation inference — an instruction to the jury that the lost e-mails were presumably relevant and damaging to defendant's case — which ultimately led to a \$29.3 million judgment against UBS.

Other recent cases illustrate how courts do not hesitate to impose a variety of sanctions against litigants who fail to abide by their discovery obligations. In 2006, the Federal District Court for the Southern District of California imposed sanctions against a defendant, an investor in Napster, Inc., in a copyright infringement action regarding musical compositions.³ After learning that the defendant's employees routinely deleted e-mails pursuant to its “long-standing”

² Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).

³ UMG Recordings, Inc. v. Hummer Winblad Venture Partners (In re Napster, Inc. Copyright Litig.), 462 F. Supp. 2d 1060 (D. Cal. 2006)

COUGHLIN DUFFY LLP

document policy, without regard to whether the deleted e-mails were relevant to the litigation, the court issued a preclusion of evidence order, an adverse inference instruction, and an award of attorneys' fees. The court found these sanctions appropriate despite the fact that the defendant's conduct did not constitute a "pattern of deliberately deceptive litigation practices," and notwithstanding evidence that the number of e-mails actually lost was small.

A New Jersey federal court imposed significant sanctions against an ERISA class action defendant for repeated e-discovery abuses, including failing to search e-mails and permanently losing others due to standard e-mail retention practices.⁴ While reserving its decision as to the propriety of a default judgment until certain class action issues had been resolved, the court, notwithstanding its proclaimed reluctance to sanction parties, issued a variety of sanctions, including: (1) deeming certain facts admitted by defendant for all purposes; (2) precluding evidence that was not produced by the defendant in discovery; (3) striking various privilege assertions by the defendant; (4) directing the payment of substantial costs and attorneys' fees related to defendant's misconduct; (5) imposing fines in an amount to be determined after the court considered defendant's financial condition; and (6) appointing a discovery monitor at the defendant's expense to review defendant's compliance with the court's discovery orders.

Notwithstanding the imposition of severe civil and judicial sanctions, organizations should also be aware of the criminal liability which may be imposed upon an organization for failure to preserve documents in light of a pending litigation. The most notorious case emerged out of the fall of Enron. In Arthur Andersen LLP v. United States, the United States Supreme Court addressed the document retention practices of Arthur Andersen during the Enron investigation.⁵ The accounting firm's policy, even after the recognition of an impending

⁴Wachtel v. Health Net, Inc., 239 F.R.D. 81, 90-91 (D.N.J. 2006).

⁵Arthur Andersen LLP v. United States, 544 U.S. at 696, 699-700 (2005).

COUGHLIN DUFFY LLP

investigation and litigation, allowed for the destruction of documents which could be relevant.⁶

In that case, the continued destruction of documents in the face of knowledge of an impending investigation and litigation led to the criminal indictment of Arthur Andersen.⁷

These cases provide examples of how electronic discovery issues can lead to extraordinary and unforeseen adverse results to litigants. Lawyers have long struggled in the paper world with the question of whether they preserved and produced everything in discovery. In the era of electronic discovery this struggle is much more challenging. Electronically stored information is easily created, however, it is also easily destroyed and/or misplaced. Locating and accounting for all your electronic data is no easy task and a source of common mistakes. Preservation orders and common law preservation obligations can be difficult to comply with when dealing with electronic data and emerging technologies.

In response to the increasing number of cases, and escalating number of sanctions and judgments involving the exchange of electronic data during litigation, the Federal Rules of Civil Procedure (“Rules”) were amended to specifically address litigant’s rights and responsibilities with regard to electronically stored information (“ESI”).⁸ Although litigants were previously obligated to preserve and produce electronic documents, the Rules now explicitly outline concerns and issues that are specific to ESI, which were necessarily not at issue when individuals were strictly confined to paper documents. The task of ESI preservation, and its impact on the litigation process, is daunting in that it includes a wide-range of information which previously did not exist or was unavailable.

⁶ Id. at 700-01.

⁷ Id. at 702.

⁸ The Rules were amended on December 1, 2006, and will be amended again effective December 1, 2007. Though the 2007 amendments make no substantive changes to the Rules, the organization and format of the Rules will change. Any citations to the Rules in this paper will be first to those currently in effect, and then to the form of the Rule in effect as of December 1, 2007.

COUGHLIN DUFFY LLP

This paper provides an overview of the recent amendments to the Rules with regard to the discoverability of ESI and the impact the changes have on litigants and potential litigants. The paper addresses when the obligations to preserve ESI arises in the context of litigation or potential litigation, the obligations that a party has with regard to preserving ESI and the legal consequences of non-compliance. Finally, we present a guide for organizations to consider in response to the newly revised Rules with regard to their individual corporate document retention policies.

II. What is Electronically Stored Information (“ESI”) and Where Do You Find It?

A. ESI Is Everywhere

The source of the trepidation from ESI preservation and the impact it has on the discovery process is the wide-range of information it encompasses which previously did not exist or was unavailable. Digital or electronic information can be stored in many different ways. When most people think about ESI, they generally look at it from the perspective of typical business documents such as e-mail, word processing documents, or spreadsheets. ESI that may be relevant to specific litigation, however, may be found in many different forms and places. Most organizations may not even be aware of where all its ESI is maintained. In recommending adoption of the revised Federal Rules the Report of the Judicial Conference Committee on Rules of Practice and Procedure said:

The discovery of electronically stored information raises markedly different issues from conventional discovery of paper records. Electronically stored information is characterized by exponentially greater volume than hard-copy documents. Common cited current examples of such volume include the capacity of large organizations’ computer networks to store information in terabytes, each of which represents the equivalent of 500 million typewritten pages of plain text, and to receive 250 to 300 million e-mail messages monthly. Computer information, unlike paper, is also dynamic; merely turning a computer on or off can change the

COUGHLIN DUFFY LLP

information it stores. Computers operate by overwriting and deleting information, often without the operator's specific direction or knowledge. A third important difference is that electronically stored information, unlike words on paper, may be incomprehensible when separated from the system that created it. These and other differences are causing problems in discovery that rule amendments can helpfully address.

The most common form of ESI at issue in litigation is e-mail since it is used universally and is often not used carefully. The content of e-mail may be very informal and subject to differing interpretations. It also is not confined to a single source. In fact, e-mail can be located almost anywhere. It may be found on company e-mail servers, e-mail backup tapes, general server backup tapes, individual PCs used by company employees, personal PCs used by employees who do work at home, Blackberrys, Personal Digital Assistant (PDA) devices, servers of external e-mail or Internet Service Providers (ISP), ISP archive tapes, printed pages, or individual storage devices such as USB drives. In addition to the location of the sender's e-mail, businesses must consider where the recipient's e-mail is being stored. For example, e-mail that is forwarded, copied, or blind copied, can end up on the same list of devices noted above for many different individuals or entities. Importantly, even if deleted, e-mail may still be recoverable and, therefore, discoverable.⁹

In addition to e-mail, ESI covers the entire range of documents that can be produced with a personal computer. This includes but is not limited to, processing files, spreadsheet files, and presentation files. Digital files, including pictures, scanned images, and video or audio recordings, can be found on the same devices and storage media listed above for e-mail. As with

⁹ Courts have ruled that Rule 34 requests seeking "deleted" electronic files are permissible. See, e.g. Antioch Co. v. Scrapbook Borders, Inc., 210 F.R.D. 645, 652 (D. Minn. 2002) (deleted computer records, including e-mail, are discoverable); Simon Property Group L.P. v. MySimon, Inc., 194 F.R.D. 639, 640 (S.D.N.Y. 2000) (court allowed the discovery of deleted files by ordering the appointment of an expert to make copies of the defendant's hard drives to extract the deleted files); Playboy Enterprises v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) (court permitted plaintiff's request for an expert to make a "mirror image" copy of the hard drive, which it would then use to locate the deleted files).

COUGHLIN DUFFY LLP

e-mail, the devices and media containing digital files may be controlled or owned by many different individuals or entities. Although digital files are easily copied, modified, and transferred, similar to e-mail, actual permanent deletion of these files is not easy and often will leave traces of the deletion activity.¹⁰

Other categories of ESI to be considered in planning discovery include company data repositories. These are typically databases containing business information, such as accounting records, personnel records, payroll records, manufacturing and sales records, mailing lists, customer lists, or any other large quantity of information that a company needs or wants to retain and use over time. Businesses should also consider fax server or fax machine logs, network system records (which maintain an extensive record of all activity performed on a computer network and on individual PCs connected to the network), company and individual voice mail systems and telephone answering devices (which may contain phone messages for long periods of time), and individual PC operating system logs (which maintain similar data as network system records although the level of detail is generally not as extensive). Also, instant messages (“IM’s”) are becoming as important and prevalent as e-mail. A party must be aware that IM’s are discoverable ESI. Of course, company security systems will generally have a record of date, time, and the entry code or ID code used by the individual making an entry and a Global Positioning System in cell phones and automobiles will also track usage.

¹⁰ See Thompson v. United States HUD, 219 F.R.D. 93 (D. Md. 2003) (stating that searching for deleted electronic records can be particularly time consuming and expensive given the number of storage locations that may have to be checked (e.g., desk-top computers, laptops, PDA's, employee home computers, back-up and archival data, and systems files, for instance), coupled with the possible need to use special search methods to locate deleted files).

B. Don't Forget the Metadata

Every document, whether electronic or not, also has a history. The history includes, but is not limited to the date of creation, the author(s), the revisions and modifications made, whether it has been copied or deleted and by whom. Prior to the advent of computers, the history of a document remained with the person(s) who created it. With technological advances and the pervasive exchange of electronic documents, however, this once private history may now be known and visible to all as metadata.

Metadata is ESI, typically not visible from the face of the document as printed out or as initially shown on the computer screen, but which is embedded in the software and retrievable by various means. It often provides information regarding the creation and modification of a document, and sometimes may include comments by persons participating in the creation or modification of the document. Under the amendments to the Rules, parties are required to consult at the onset of the litigation about the nature of pertinent electronic documents in their custody and the manner in which they are obtained.¹¹ During these initial discussions, an issue which will likely be raised is how the parties will handle the metadata contained in documents. This includes whether the parties wish to obtain the metadata, and if so, whether there will be any assertion or claim of privilege over some or all of the metadata.

Metadata raises unique issues concerning the waiver of privileges and whether it is ethical to remove metadata unbeknownst to other parties in litigation. One issue is whether metadata included in ESI can be scrubbed or deleted prior to producing the ESI. Another is whether a party can produce files by converting them to hard copy, scanning them, and then sending the image to the requesting party. Because metadata can provide important and critical information in certain instances and may also be considered probative evidence in litigation, it is

¹¹ F.R.C.P. 26(f)(2006), F.R.C.P. 26(f)(2007)

COUGHLIN DUFFY LLP

wise not to either scrub metadata or produce images of documents without the agreement of either the requesting party or the court.

In fact, the scrubbing or altering of the metadata, absent such consent, may expose a party to discovery sanctions.¹² In Williams v. Sprint United Management, the defendant produced requested spreadsheets but scrubbed the metadata. The court had ordered that the spreadsheets be produced in the form in which they are ordinarily kept. As a consequence, the court ordered the reproduction of the spreadsheets with the metadata. It also ordered that any assertion of privilege with regard to the metadata was deemed waived. In In re Seroquel Products Liability Litigation,¹³ 2007 U.S. Dist. LEXIS 61287 (M.D. Fl. August 21, 2007), the defendant in a multi-district pharmaceutical products liability litigation was found by the court to have turned over ESI in unreadable formats. The plaintiffs had requested a large volume of ESI and the defendant produced over 10 million pages in electronic format. The scrubbing of metadata was a component of these issues. As a result, the court sanctioned the defendants, allowing the plaintiffs a further hearing to present evidence on their damages caused by defective production by the defendant.

C. Metadata and the Inadvertent Disclosure of Attorney-Client Communications and/or or Confidential or Proprietary Trade Secrets

The larger the amounts of electronic material that are produced in native format, the greater the odds that privileged content and/or metadata will get disclosed. Ethical obligations and case law exist to mitigate the ramifications of an inadvertent disclosure. As a practical matter, however, once privileged matter has been disclosed to an adversary or the public the

¹² Williams v. Sprint United Mgt., 230 F.R.D. 640 (D. Kan. 2005) (court required the production of metadata as probative evidence); but see Kentucky Speedway, L.L.C. v. NASCAR, Inc., 2006 U.S. Dist. LEXIS 92028 (E.D. Ky. December 18, 2006)(court found there was a presumption against the production of metadata and that the requested metadata was not relevant).

¹³ In re Seroquel Products Liability Litigation, 2007 U.S. Dist. LEXIS 61287 (M.D. Fl. August 21, 2007).

COUGHLIN DUFFY LLP

recipient will not be able to erase it from his/her memory. The inadvertent disclosure of metadata is one of the biggest risks facing lawyers today -- a risk made more acute by ethical and professional requirements to safeguard client confidences.

Generally speaking, the dangers of producing privileged or confidential information exist in two contexts. First, issues may arise in connection with an attorney's communications with a client's adversaries or third parties. Second, risks arise during the disclosure of a client's underlying documents and communications in the course of litigation. In either circumstance, inclusion of metadata in the document provided could accidentally expose confidential information to the detriment of the client and the attorney-client relationship. In recent years there has been a series of diverging ethics opinions among different jurisdictions in the United States regarding an attorney's ethical responsibilities with respect to the handling of metadata in electronic documents. For example, the August 2006 Formal Opinion 06-442 of the American Bar Association states that the "the Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party." Similarly, the Maryland State Bar Association Committee on Ethics found that "there is no ethical violation if the recipient attorney (or those working under the attorney's direction) reviews or makes use of the metadata without first ascertaining whether the sender intended to include such metadata."

In contrast, the New York State Bar Association Committee on Professional Ethics issued an opinion finding that lawyers had an ethical duty to try to limit improper disclosure of metadata pursuant to DR 4-101(B), which states that a lawyer shall not "knowingly" reveal a

COUGHLIN DUFFY LLP

client's confidences or secrets.¹⁴ The opinion noted that metadata may, among other things, include editorial comments, strategy considerations, legal issues raised by the client or lawyer, and legal advice provided by the lawyer. Although not all metadata is necessarily confidential or secret, the committee noted that it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client. Therefore, the committee explained, when a lawyer sends a document by e-mail, as with any other type of communication, the lawyer must exercise reasonable care to ensure that she does not inadvertently disclose her client's confidential information. The committee stated that what constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document and the identity of the intended recipients of the document. Significantly, the committee found that reasonable care may, in some circumstances, call for lawyers to stay abreast of technological advances.

Similar to the approach taken by the New York Bar Association, in August 2007, the Legal Ethics Committee of the District of Columbia Bar issued Ethics Opinion 341. The DC Bar's opinion concluded that "when a receiving lawyer has actual knowledge that an adversary has inadvertently provided metadata in an electronic document, the lawyer should not review the metadata without first consulting with the sender and abiding by the sender's instructions. In all other circumstances, a receiving lawyer is free to review the metadata contained within the electronic files provided by an adversary."

In a recent case involving inadvertent disclosure of information embedded in the metadata, the United States Federal Trade Commission ("FTC") released dozens of trade secrets

¹⁴ New York Bar Association Opinion Number 782 (Dec. 8, 2004)

COUGHLIN DUFFY LLP

in public court documents involved in an antitrust litigation to block Whole Foods Market's \$565 million purchase of Wild Oats.¹⁵ The FTC documents revealed that Whole Foods planned to close 30 or more Wild Oats stores in competitive markets, a move that the company believed would nearly double revenue for some Whole Foods stores. In addition, the FTC documents disclosed how Whole Foods negotiates with suppliers to drive up costs for stores. In the documents, the FTC regulators also discussed the company's closely held marketing strategies. Many of the details in the documents, which FTC lawyers filed electronically, were not intended to be released publicly, but words which were believed to be redacted were actually just electronically shaded black. In fact, the words could be searched, copied, pasted and read in versions downloaded from court computer servers. Court officials did realize the mistake and replaced the filing with a version using scanned pages of the redacted documents. However, the Associated Press downloaded the document from the public server before it was replaced by a properly redacted version. As a result, confidential and proprietary trade secrets of Whole Foods were disclosed to the public.

Given the undeveloped nature of the law, continually evolving technology, the exponential dependence on electronic communications, and the potentially catastrophic impact of inadvertent disclosure of a client's secrets or confidence, it is clear that the issue of metadata protection is likely to continue to plague unwary lawyers and their clients and inflate the cost of transaction and litigation representation. Therefore, it is vital for corporations and their counsel to be aware of metadata and of how their software stores it in order to properly safeguard their clients' confidences. In addition, there must be a continuing dialogue among lawyers, their clients and the client's IT departments to ensure that the disclosure of metadata that is potentially

¹⁵ Christopher S. Rugaber, *Error by FTC Reveals Whole Foods' Trade Secrets*; Associated Press, August 15, 2007 at <http://www.washingtonpost.com/wp-dyn/content/article/2007/08/14/AR2007081401784.html>

privileged and/or confidential is protected. As the Williams and Seroquel cases illustrate above, parties are not free to determine on their own whether to keep or scrub metadata. While metadata may not be probative or relevant in all cases, it is difficult to determine if this is so at the outset of, or prior to, litigation. Therefore, it is prudent for companies to avoid scrubbing metadata included in litigation holds to avoid the possible consequence of sanctions. Instead, parties should determine whether they might want to scrub metadata, and then, when conferencing with their adversaries after the inception of litigation, attempt to agree on what metadata will or will not be produced. In the event that the parties cannot come to a mutual agreement as to the treatment of the metadata, they can always resort to the assistance of the court to resolve the matter.

III. The Impact of the Changes to the Federal Rules of Civil Procedure on Your Organization

Contrary to the suggestions in the legal media, the amendments to the Federal Rules do not alter or change any previous obligations of litigants in connection with anticipated or pending litigation. Instead, the amendments are intended to clarify and outline a litigant's obligations regarding ESI. While reasonably clear prior to 2006, the revised Rules make it resoundingly clear that ESI is not only discoverable in all of its forms, but that potential parties to litigation have a responsibility to preserve that information. In conjunction with the amendments to the Rules, individual states within the United States have also begun updating their discovery rules. For example, California has authorized its courts to order parties to produce discovery electronically.¹⁶ Illinois, Mississippi, New Jersey and Texas courts allow parties to request ESI

¹⁶ CAL. CIV. PROC. CODE §§ 2017.710-2017.740 (2007).

COUGHLIN DUFFY LLP

in specific forms.¹⁷ In addition, Kansas and Wyoming now require attorneys to be familiar with their client's computer systems.¹⁸

Businesses, therefore, must be concerned with three crucial questions regarding the discovery of ESI:

- (1) What events may trigger an obligation to preserve ESI? This entails determining the likelihood of potential court action, and whether, and when, the party in question should have known of the likelihood of court action;
- (2) What types of documents should be preserved? Is the data "relevant"? This is not a straightforward question because it depends on the facts of every individual case, and is an inherently subjective question. If the data is relevant, then a potential party has the duty to preserve that data; and
- (3) Once the litigation has begun, and data is requested, does the requesting party have a right to the data? Should the requesting party pay for the expense of getting the data?

A. The Duty to Preserve Information: Litigation Hold Letters

With the wide-range and volume of data currently being stored electronically, organizations may face a daunting challenge when a legal obligation arises to preserve documents. Absent reasonable notice of impending litigation, the Rules impose no sanctions or other penalties on litigants who destroy documents in the normal course of business.¹⁹ Once litigation can be reasonably anticipated, however, any automatic deletion programs must be terminated.²⁰ Though not a new requirement,²¹ in light of the amendments to the Rules and recent court opinions imposing sanctions on parties for their failure to preserve and/or produce electronic documents, an effective internal litigation hold letter is critical for an organization

¹⁷ See Douglas W. Kim, *E-discovery: A Practical Approach*, The SciTech Lawyer, Fall 2007, at 7.

¹⁸ *Id.*

¹⁹ F.R.C.P. 37(f)(2006); F.R.C.P. 37(e)(2007).

²⁰ *Peskoff v. Faber*, 2007 U.S. Dist. LEXIS 62595 at *20 (D.D.C. Aug. 27, 2007).

²¹ *Lewy v. Remington Arms Co. Inc.*, 836 F.2d 1104 (8th Cir. 1987).

COUGHLIN DUFFY LLP

threatened with litigation. The recent revisions to the Rules and the increasing number of e-discovery judicial opinions may lead some to believe that preservation obligations with regard to electronic discovery are a new concern. However, courts, as well as advisory and regulatory bodies, have long required that parties and their employees, agents and/or representatives in possession of relevant evidence in any form should safeguard the preservation of that evidence.²²

One of the earliest cases to discuss the obligation to preserve documents in light of the emergence of electronic media was the seminal case of In re Prudential Ins. Co. of Am. Sales Practices Litigation.²³ The Prudential case brought to the forefront the inherent problem facing companies in connection with ensuring that its relevant electronic documents are preserved in connection with anticipated or pending litigation. This policyholder class action lawsuit stemmed from allegations that Prudential employed deceptive sales practices in its sale of life insurance policies.²⁴ The federal district court entered a discovery order early in the case requiring all parties to preserve all documents and “other records” relevant to the litigation. Despite this order, documents were destroyed at four Prudential offices. Although Prudential management had distributed document retention instructions to its agents and employees via its e-mail system, some employees did not have access to e-mail, while others routinely ignored it. Furthermore, senior management never distributed the court’s directive to all of its employees. As a result, outdated sales practice records – key records pertinent to the lawsuit – were destroyed by Prudential. In light of the foregoing, the court held that Prudential lacked a “clear

²² See The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery I (Sedona Working Group Series 2004); Sedona Conference, the Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age, [available at www.thesedonaconference.org](http://www.thesedonaconference.org).

²³ In re Prudential Ins. Co. of Am. Sales Practices Litigation, 169 F.R.D. 598 (D.N.J. 1997).

²⁴ Id. at 600.

and unequivocal document preservation policy,” that the lost materials were relevant and would have reflected negatively on Prudential, and imposed a \$1 million sanction.²⁵

1. What triggers an organization’s obligation to issue a Litigation Hold Letter or Preservation Notice?

There are obvious events that trigger the issuance of a litigation hold letter, such as the filing of a complaint (on your own behalf or by another party), a form notice of claim, receipt of a subpoena or knowledge of a civil or criminal investigation by a regulatory or government agency.²⁶ Notwithstanding, there are many other events that can predate the filing of a complaint, or notice of an ensuing investigation, that may place an organization on “notice” of potential litigation, warranting the issuance of a litigation hold letter or preservation notice. In fact, courts have held that the “obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party *should have known that the evidence may be relevant to future litigation.*”²⁷ In this regard, once a party reasonably anticipates litigation, including litigation it plans to initiate, courts have held that it is under an obligation to suspend its routine document retention/destruction policy and put in place a “litigation hold” to ensure the preservation of relevant documents.²⁸ Unfortunately, neither the Rules nor courts have set clear and exact guidelines describing precisely when, prior to the filing of a complaint,

²⁵ In the ten years following the Prudential decision, a large number of courts have held that senior management in organizations have an obligation to effectively distribute a litigation hold notice to its employees. See e.g., Danis v. USN Communications, Inc. No. 98 C 7482, 2000 WL 1694325, at 38-41 (N.D. Ill. October 20, 2002) (circumstances of the case indicated insufficient involvement of management in proper oversight and delegation of preservation responsibilities).

²⁶ Procter & Gamble Co. v. Haugen, 2003 WL 22080734, No. 1:95CV94 DAK (D. Utah August 19, 2003)

²⁷ Zubulake v. UBS Warburg, L.L.C., 220 F.R.D. 212 (S.D.N.Y. Oct. 22, 2003) (“Zubulake IV”) (emphasis added); See also, The Sedona Conference, Commentary on Legal Holds, the Trigger & the Process, Sedona Conference Working Group on Electronic Document Retention & Production (WG1) (August 2007 Public Comment Version), Guideline 1 “Reasonable anticipation of litigation arises when an organization is on notice of a credible threat it will become involved in litigation or anticipates taking action to initiate litigation,” available at www.thesedonaconference.org.

²⁸ Id.

COUGHLIN DUFFY LLP

the duty to preserve data begins.²⁹ Since a party can be sanctioned if it fails to preserve data when it should, it is of paramount importance that potential parties be aware when they must cease automatic deletion programs and begin retaining ESI.³⁰

While there may be some mystery about when to impose a litigation hold, in many cases there is no need for potential parties to guess at whether litigation may ensue. If some employees think that a fellow employee, client, or other third party, may sue, this conjecture does not create an obligation to preserve data.³¹ However, if a potential party begins internal discussions about how to handle future litigation, or begins creating new documents or data for the purpose of potential litigation, then a data preservation program must be created.³² Unfortunately, this is not a precise science, as illustrated below.

In the leading case of Zubulake v. UBS Warburg, L.L.C., the defendant, one of Europe's largest financial services firm, was sued in a gender discrimination action in August of 2001. Yet the court determined that the defendant's obligation to preserve documents began in April of that year. The court based its determination on two facts. First, the defendant's employees began discussing the plaintiff in e-mails which were entitled "UBS Attorney Client Privilege." Second, the director of the firm's U.S. Asian Equities Sales Desk, who was the plaintiff's direct superior and one of the individuals who allegedly discriminated against the plaintiff because of her gender, testified that as early as April of 2001 he thought a potential lawsuit was possible. The Zubulake court found that because almost all the defendant's employees were circulating e-mails about potential litigation and the plaintiff's direct superior also thought litigation was possible, the defendant was on notice as early as April of 2001 of potential litigation. In fact, the

²⁹ Cache La Poudre Feeds, L.L.C. v. Land O'Lakes, Inc., 2007 U.S. Dist. LEXIS 15277 at *24 (D. Co. March 2, 2007) (stating that the time when the duty to preserve ESI arises is determined on a case by case basis).

³⁰ See *infra* Section IV.

³¹ Zubulake IV, 220 F.R.D. at 217.

³² Samsung Elecs. Co. v. Rambus Inc., 439 F. Supp. 2d 524, 542 (E.D. Va. 2006).

COUGHLIN DUFFY LLP

court determined that the idea that litigation was possible was “pervasive”, and was held by a senior official in a decision making position. This combination of facts led the Zubulake court to conclude that the defendant should have reasonably anticipated litigation, and begun a document preservation program, i.e. litigation hold prior to the plaintiff’s formal filing of a complaint.³³

The two key concepts that emerged from Zubulake that potential parties should keep in mind when determining whether to impose a litigation hold are: 1) *probability* and 2) *reasonableness*.³⁴ Potential parties must conclude that litigation is likely, not a mere possibility, before a litigation hold becomes necessary. The conclusion that a party reaches as to probability must also be reasonable, i.e., the party must have evidence to which it can point that supports its conclusions about probability. Despite the fact that it is impossible to say where parties can draw the line on the imposition of litigation holds, what follows is a short list of events that should lead to the imposition of a litigation hold:

- A draft complaint, whether filed or not;
- Requests for production of documents;
- A subpoena from a third party;
- A request to preserve specific documents;
- A complaint filed with or by a regulatory agency;
- A written demand letter from a lawyer for a party that makes a claim and proposes a resolution, clearly threatening litigation if no resolution is reached.

If litigation is threatened or a party receives a demand letter, that party should ask the following questions:

- How specifically do the communications with the other party describe the circumstances which led to the demand? Are the specifics correct?
- How credible is the demand?
- Who authored the demand letter, and what is his/her role?

³³ Zubulake IV, 220 F.R.D. at 216-17.

³⁴ TODD L. NUNN, ET AL., UNDERSTANDING THE NEW E-DISCOVERY RULES 20 (DRI 2006).

COUGHLIN DUFFY LLP

- Who is the communicator for the other party and to whom are they writing? Is the communication to or from attorneys?
- How explicit and credible is the threat of litigation?

The duty to impose a litigation hold can also come from a third party source, such as a news media report. To determine if a litigation hold should be imposed based on such sources, parties should ask:

- How reliable and accurate is the source?
- How widespread are such reports?

On the other hand, if you are the party contemplating litigation, you should ask yourself the following questions:

- Who within your organization knows anything about the proposed litigation? Does that individual have authority to sue? If not, have they told any decision-maker(s) about the facts which form the basis of the suit?
- Does legal counsel, whether in-house or outside counsel, know the facts and been asked for an opinion?
- Have any steps been taken towards filing suit, or communicating with other parties about the potential suit?
- Has there been any research on a demand letter or has one been sent?³⁵

The determination of the timing of pre-litigation preservation decisions requires a fact-sensitive analysis. Indeed, an organization may have to make a decision to preserve documents years before an actual lawsuit is instituted.³⁶ Therefore, if after considering the facts at issue, the parties involved, the relationship between the parties and the potential for the dispute to rise to the level of a formal complaint, an organization is seriously considering whether documents may

³⁵ Id. at 21.

³⁶ Zubulake IV, 220 F.R.D. at 216-17 (S.D.N.Y. 2003) (UBS reasonably anticipated litigation five months before the filing of the EEOC charge (and a few years prior to the filing of a civil complaint) based on the e-mail of several employees revealing that plaintiff intended to sue); Stevenson v. Union Pac. Ry. 354 F.3d 739 (8th Cir. 2004) (railroad reasonably knew that fatal crashes usually lead to litigation).

require preservation in connection with anticipated litigation, then chances are a litigation hold letter or preservation notice is warranted.

2. The Essential Elements of an Effective Litigation Hold Letter

Once an organization makes a determination that it is under a duty to preserve documents, it must notify its employees in writing, detailing what types, and for what time period, documents must be preserved. A litigation hold letter or preservation notice, serves the purpose of directing a party to protect from destruction certain documents and data that are, or could possibly be, relevant to a threatened or pending litigation, regulatory investigation or audit.

One commentator has defined the litigation hold letter as:

...a written directive to all potentially relevant personnel of a company advising them that there is a specific subject matter which has resulted or is likely to result in litigation, to describe that subject matter, and the people involved in it, in sufficient degree to inform the recipients of the communication of the true nature of the actual or anticipated dispute, and then to specifically advise them to both locate and save all relevant paper documents, e-mails, and any other items that may be contained in the company's computer system.³⁷

In drafting an effective litigation hold letter, organizations must be aware that this letter must be read and understood not only by employees or third parties but perhaps by adversaries and the court should the matter evolve into litigation. In fact, the letter must be understood by a broad corporate audience, from the mailroom to the board room while at the same time contain the necessary elements required by courts to ensure that organizations have taken all necessary steps to comply with any discovery obligations. Therefore, the key is to craft a letter that is straightforward and simple yet maximizes compliance and thereby reduces the risk of evidence

³⁷ Timothy J. Hagan, *The International and Domestic Implications of Electronic Discovery on Litigation and Business Practices*, International Legal News, vol. 2 at 7 (June 10, 2005).

COUGHLIN DUFFY LLP

destruction. In order for the letter to be effective the following guidelines should be followed in drafting an internal litigation hold letter:

1. **The letter should be sent by high level corporate officers such as the company Chairman, Chief Operating Officer or General Counsel.** This emphasizes that the obligation to preserve documents is recognized as important by the highest levels of the company and that company management is aware of and endorses the process. As the Prudential case made clear this obligation cannot be delegated in any event.
2. **It should be sent to the appropriate corporate audience.** It is not necessary, especially in larger corporations, for the litigation hold letter to be directed to all employees. However, it is vital that the letter be disseminated to those employees and departments that could potentially have access to relevant information. When the issues in dispute have not been clearly defined or the company is unaware of all the potential issues that may arise, it is advisable to err on the side of broader dissemination.
3. **It should be simple and straightforward.** In order to ensure that employees will read and understand the mandate to preserve documents, an internal hold letter should not exceed five or six brief, plainly worded, and easily understood paragraphs. The first or second paragraph of the letter should simply and clearly tell the employee what the subject matter at issue is, the nature of the litigation or investigation and that all documents and data, electronic or otherwise, relating to that issue, should be carefully preserved.
4. **It must define what needs to be preserved and where it might be located.** This is likely one of the most important elements to the letter. The hold letter should define the term “documents and data” and the potential “sources” of where the data may be stored, in order for the employee to understand the broad scope of the obligation. More importantly, this reminds the employee that documents are not relegated merely to paper documents but include a wide-range of electronic documents and sources, including back-up tapes.

COUGHLIN DUFFY LLP

5. **It must give clear direction to the audience.** Employees must be made aware of exactly what steps need to immediately take place in order to ensure the proper preservation of documents.
6. **Inform and identify for the audience the risks of non-compliance.** Employees must also be made aware of the importance of preserving documents and the risks or serious consequences to the company if the data is intentionally or unintentionally, lost, destroyed or compromised.
7. **Advise the audience of the continuing duty to preserve documents and the company's continued follow-up.** The litigation hold letter is only effective if employees understand that this is a continuing obligation. Moreover, they must be made aware that management and its legal counsel (in-house and/or outside) will be following up on the employee's preservation efforts. There must be an established follow-up protocol. A litigation hold will only be effective if there is continuous follow-up by management and its counsel.

As evidenced by the Prudential case, having a preservation notice or litigation hold in place is not enough, it must be disseminated to all employees who could potentially have access to relevant information in connection with the pending or anticipated litigation. Because of the globalization of business, special attention should be paid to information that may be held in locations outside of the United States, where other countries may have laws that conflict with U.S. discovery requirements. For example, the European Directive 95/46/eC (the "Directive"), effective October, 1998, governs the processing and use of personal data for all EU Member States, and identifies eight data protection principles. This includes the principle that personal data shall not be kept for longer than is necessary for the purposes for which it is processed. It also states that personal data shall not be transferred to a country or territory outside of the EU, unless that country or territory ensures an "adequate" level of protection for the rights and

freedom of data subjects in relations to the processing of personal data.³⁸ Whenever the laws of the EU or individual members thereof conflict with obligations in the U.S., those questions should be put to the U.S. court to determine the proper course of action. Otherwise, if a party makes its own choice, and a U.S. court disagrees with that course of action, a party may potentially be exposed to sanctions.

An even bigger hurdle may be the underlying differences in the judicial systems. Most of Europe has adopted rules of disclosure under which parties are not typically required to produce a large volumes of documents, while in the United States, parties can request that their adversaries turn over any “relevant” documents.³⁹ There are differences among the individual nations of the EU as well. For example, it is illegal in Germany to examine e-mails an employee marks private without the permission of the employee.⁴⁰ Yet in the United States, e-mails are considered the property of the employer. When faced with litigation in the United States every party must remember that there may be different rules with which it must become familiar, some of which may conflict with the laws of the home forum. As the cases in this area demonstrate, a party’s decision whether to issue a litigation hold letter and the proper steps to affect a hold will be highly scrutinized if any evidence is alleged to have been lost during the course of a litigation.

B. The Scope of the Duty to Preserve: What Data is Potentially Relevant?

Once a potential party imposes a litigation hold, or has been served with a complaint or a demand to preserve documents, it must determine what data to retain. United States courts do not expect businesses, especially large organizations, to save every bit of data that passes through

³⁸ The Sedona Conference, Commentary on Legal Holds, the Trigger & the Process, Sedona Conference Working Group on Electronic Document Retention & Production (WG1) (August 2007 Public Comment Version), Guideline 6 “When a duty to preserve arises, reasonable steps should be taken to identify and preserve relevant information as soon as practicable. Depending on the circumstances, a written legal hold (including a preservation notice to persons likely to have relevant information) may be issued,” available at www.thesedonaconference.org.

³⁹ Matthew Blake, The Perilous Journey of Overseas E-Discovery, available at www.discoveryresources.org/pdfFiles/blake_022006.pdf.

⁴⁰ Id.

COUGHLIN DUFFY LLP

its operations, recognizing that such a requirement would cripple the business.⁴¹ Courts do require that businesses identify *what* documents are relevant, and *who* are the relevant persons. Thus, for example, in an employment discrimination case, while quarterly profit forecasts would not be relevant, e-mails most likely will be. And while e-mails may be relevant, only e-mails sent to and from relevant persons need to be preserved, rather than all company-wide e-mails.

The Rules guide the exchange of ESI after litigation has begun, requiring litigants to give the other parties any ESI that it plans to use to support its position.⁴² The Rules do allow parties to withhold from production any document which may be subject to an evidentiary privilege, such as attorney-client privilege.⁴³ Even if information subject to a privilege is turned over, the party that inadvertently released the information can demand that the party that received the information destroy any copies made and return the ESI.⁴⁴ Parties can also withhold ESI that is difficult to access, either in terms of effort or expense.⁴⁵ This ground for withholding ESI is explored more thoroughly in the next section.

Before producing ESI to another party, litigants must review what data should be released. The first step is determining where potentially relevant data may be located. ESI can be divided into five different categories:

- Active, online data, such as hard drives, which are easily accessible.
- Near-line data, usually meaning a robotic storage device which houses removable media, and uses robotic arms to access the data.

⁴¹ *Zubulake IV*, 220 F.R.D. at 217.

⁴² F.R.C.P. 26(a)(1)(B)(2006); F.R.C.P. 26(a)(1)(A)(ii)(2007).

⁴³ F.R.C.P. 26(b)(5)(A)(2006); F.R.C.P. 26(b)(5)(A)(2007).

⁴⁴ F.R.C.P. 26(b)(5)(B)(2006); F.R.C.P. 26(b)(5)(B)(2007).

⁴⁵ F.R.C.P. 26(b)(2)(B)(2006); F.R.C.P. 26(b)(2)(B)(2007).

COUGHLIN DUFFY LLP

- Offline storage or archived data, which is typically stored on a removable optical disk or magnetic tape media.
- Backup tapes.
- Erased, fragmented or damaged data.⁴⁶

Each of these categories of data must be considered when a party is investigating where potentially relevant data is located. The next step should be determining who are the “key players” in the impending or current litigation. “Key players” are those employees who are likely to have relevant information.⁴⁷ This is a critical step in the process. Determining who is a “key player” is obviously situation dependent, but should be relatively clear with each situation. For example, in Zubulake, the “key players” were Zubulake’s co-workers at the Asian Equities Sales Desk, including the head of the Desk.⁴⁸ Potential parties should err on the side of caution when making this determination as it is not worth risking possible sanctions down the road.⁴⁹ Potential parties must be proactive in this area, and “key players” who are known should be interviewed so that other “key players” can be identified.

Once the “key players” have been identified, a potential party should determine what data to preserve. Parties must preserve anything that was created by or on behalf of any of the “key players,” and any other data which refers in any way to the subject of the current or impending litigation. Further, while a party need not search inaccessible data for potentially relevant ESI, if it does know or becomes aware that potentially relevant ESI exists on inaccessible data, that data must be preserved.⁵⁰ Again, it is best to err on the side of caution when determining what data to

⁴⁶ Zubulake v. UBS Warburg, L.L.C., 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003) (“Zubulake I”).

⁴⁷ Zubulake IV, 220 F.R.D. at 218.

⁴⁸ See generally, Zubulake III, *supra*.

⁴⁹ See *infra* Section IV.

⁵⁰ Zubulake IV, 220 F.R.D. at 218.

COUGHLIN DUFFY LLP

preserve. As a rule of thumb, anything that can contain any potential relevance to an impending or current lawsuit must be preserved.

When searching for potentially relevant data, parties must look not only at the ESI within its possession, but also within its control. Thus, if a party contracts with a third party to store its data, or uses a third party to run its web servers, the information held by those third parties is under its control, and must be searched for potentially relevant data.⁵¹ In Columbia Pictures Industries v. Bunnell et al., the defendant was alleged to have infringed on the copyrights of the plaintiff by running a file sharing service over the internet, allowing users to download movies.⁵² The defendant used the servers of a third party that stored information, including movie files, that were downloaded by users.⁵³ The defendant argued that the files on those servers were not discoverable because they were not within the defendant's possession. The court rejected this argument, holding that, because the defendant had control and access to those files, it was required to preserve and produce them on request.⁵⁴ As Bunnell illustrates, the rule in this area is to leave no stone unturned. Wherever a party may store data, so long as it is accessible, and under the control or possession of that party, it must be identified, located, and searched.

Once a party has determined the "key players" and what data it must preserve, it must determine how to preserve it. Parties can choose how to preserve data identified as potentially relevant. There are some general guidelines that parties should follow when determining how to preserve the data. Making mirror image copies of the data will always be acceptable. Simply retaining the data in its present form is also acceptable. Parties should not alter data in any way,

⁵¹ See Columbia Pictures Indust. v. Bunnell et al., 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. June 19, 2007).

⁵² Id. at *8-16.

⁵³ Id.

⁵⁴ Id. at *55.

as this will likely lead to sanctions and penalties being imposed once the data is disseminated in litigation.⁵⁵ Therefore, retaining the integrity of the original document is vital.

C. Who bears the costs of producing the ESI?

Once a party is aware of how the data must be released, parties often become concerned over the cost of such productions. In fact, the cost of discovery is often the most important consideration by parties when considering entering into, and settling lawsuits. For many productions of ESI, the cost will be similar to, if not less than, the cost of a production of paper discovery. ESI is more easily searched than paper documents, and can, in many cases, be collated and stored more quickly with less man power. This is only true, however, when the data is easily accessed and searched.⁵⁶ When the data is stored on backup tapes, or on other medium which must be restored in order to be fully searched, the time and expense of producing data located on such medium can grow exponentially.

The Federal Rules allow for a party to object to producing ESI if it can demonstrate “undue burden or cost.”⁵⁷ For the most part, even if a party can show that producing the requested ESI will impose too great of a burden or cost, courts will still order the production, although they may shift the cost of that production to the party requesting the data. Parties must remember that courts will not shift the cost of production in every case.⁵⁸ Courts first apply a seven part test to determine whether the request imposes an undue burden or cost, making cost shifting appropriate:

1. How specifically does the request ask for ESI that will likely be important in the litigation?

⁵⁵ See *infra* Section IV.

⁵⁶ See *supra* text accompanying note 46.

⁵⁷ F.R.C.P. 26(b)(2)(C)(2006), F.R.C.P. 26(b)(2)(B)(2007).

⁵⁸ Zubulake I, 217 F.R.D. at 318.

COUGHLIN DUFFY LLP

2. Can the ESI being sought can be obtained from other sources?
3. How much will the production cost, compared to the amount of damages the plaintiff claims?
4. How much will the production cost, compared to the cost of production with the resources available to each party?
5. What is each party's ability to produce the data as cheaply as possible, and what is their incentive to do so?
6. What issues will the data go to, and how important are those issues in the litigation?
7. What are the relative benefits to each party of getting the information?⁵⁹

The most important factors a court will look at are the specificity of the request and whether the information can be obtained from any other source. What courts are looking for is the likelihood that the requested discovery contains the data sought. The more likely it is that the ESI has the information desired, the more likely it is that courts will require the responding party to pay the cost of the production.⁶⁰ If a court determines that there is a low probability that the requested ESI does not contain the information sought, then it will look at the next three factors, which seek to answer the questions of how expensive the production will be and which party is in the best position to handle the cost.⁶¹ The remaining factors are of relatively little importance and rarely come into play.⁶²

⁵⁹ Id. at 322, see also Notes of the Advisory Committee on 2006 Amendments (“Advisory Committee Notes”), F.R.C.P. 26.

⁶⁰ McPeck v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001).

⁶¹ Zubulake I, 217 F.R.D. at 323.

⁶² Id.

COUGHLIN DUFFY LLP

Following this analysis, courts have come to different conclusions about when to order a requesting party to bear the cost of production. Some courts will order a limited production, or “sampling”, to determine what, if anything, will be found. Only if, after the “sampling”, it appears that a further search is of any utility, will a complete production be ordered.⁶³ Other courts will order the production, but shift only a portion of the cost to the requesting party.⁶⁴ Some courts will shift the entire burden to the requesting party, when the disparity between the resources of the two parties is great, and the chances that the sought after data exists in the requested ESI. While the seven factor test has no presumption either for or against cost shifting, in practice, there must be quite a low likelihood that the requested ESI contains the sought after data, and a large disparity between the resources of the parties, for a court to order a total shifting of cost. Responding parties must be aware that they will likely still shoulder quite a bit of the cost for any requested production. Notwithstanding, they should also be aware that the cost of the production is less than that of any sanctions that may be imposed for not producing, or altering, the requested ESI.

D. Post-Litigation Procedures

While the Rules explain in what form ESI can be produced, parties are encouraged to come to their own agreements about how ESI may be produced.⁶⁵ When a request for the production of ESI is made, the requesting party can ask that the ESI be turned over in a specific form.⁶⁶ The party receiving the request can object to the requested form of the ESI, but must give reasons why it is objecting and what form it intends to use.⁶⁷ If no specific form of ESI is

⁶³ Hagemeyer N. Am., Inc. v. Gateway Data Scis. Corp., 222 F.R.D. 594, 603 (E.D. Wisc. 2004).

⁶⁴ Zubulake v. UBS Warburg, L.L.C., 216 F.R.D. 280, 289 (S.D.N.Y. 2003) (“Zubulake III”); see also Wiginton v. C.B. Richard Ellis, Inc., 229 F.R.D. 568, 577 (N.D. Ill. 2004).

⁶⁵ Parties are encouraged to discuss discovery of ESI during the discovery-planning conference and reach agreement on the forms of production. Advisory Committee Notes, F.R.C.P. 26(f).

⁶⁶ F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(1)(C)(2007).

⁶⁷ F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(2)(D)(2007).

COUGHLIN DUFFY LLP

requested, and there is no agreement between the parties governing the form of ESI to be produced, then a party which is producing ESI must produce it in the form in which it is usually maintained, or a form that can be used by the requesting party with relative ease.⁶⁸

Pitfalls, however, abound when producing ESI absent an agreement on the form of the production. Courts will not hesitate to penalize parties who attempt to gain an advantage by producing ESI in a manner which is difficult for the other parties to use. Even production of ESI in paper form is not always appropriate. In In re Bristol-Myers Squibb Securities Litigation,⁶⁹ the parties agreed on a ten cents per page charge for copies during discovery.⁷⁰ The court vacated the agreement, however, upon the revelation that the defendant was producing electronic documents in paper form.⁷¹

While the Rules mandate a pre-trial conference between the parties and a judge to arrange for a schedule of discovery, the parties are encouraged to make their own arrangements prior to this meeting. The best way to prepare for such meetings is to meet with a representative from the Information Technologies department in order to become more familiar with the terminology and technology at issue. It is also a good idea to plan on deposing a representative of the other party's Information Technology department, so that the ESI received from that party can be used in the most efficient and productive way.

IV. Consequences of Non-Compliance

Failure of a party to abide by the discovery obligations, may give rise to legal and economic sanctions. Potential sanctions for non-preservation or spoliation include: dismissal of claim or granting judgment in favor of a prejudiced party, suppression of evidence; and adverse

⁶⁸ F.R.C.P. 34(b)(2006); F.R.C.P. 34(b)(2)(E)(2007)

⁶⁹ 205 F.R.D. 437 (D.N.J. 2002).

⁷⁰ Id. at 439.

⁷¹ Id. at 440-41.

COUGHLIN DUFFY LLP

inference or spoliation inference; fines, and attorneys' fees and costs. In addition, courts may order the re-production of ESI if the initial production is not in the proper form. While not a sanction per se, the cost of production can be staggering. By one estimate, a typical hard drive storing up to 9,000,000 pages cost more than \$1,000,000 to produce.⁷²

There are many examples of the consequences to companies who fail to comply with the obligations arising from the preservation of electronically stored information. For example, in Coleman Holdings v. Morgan Stanley & Co., a \$1.45 billion verdict was entered against Morgan Stanley arising from its inability to recognize substantial shortfalls in e-mail production when it represented that all responsive e-mails were produced.⁷³ In response to the plaintiff's initial request for discovery, Morgan Stanley produced only 8,000 pages of documents, including only a handful of e-mails.⁷⁴ The court ordered Morgan Stanley to preserve ESI and do a more thorough search of its records.⁷⁵ After certifying that it had complied with the order, Morgan Stanley revealed that it had discovered about 1,000 backup tapes which had not previously been disclosed.⁷⁶ As a consequence, the court ordered that the burden of proof at trial would be shifted from the plaintiff to the defendant, and a statement to the jury of Morgan Stanley's efforts to hide its e-mails.⁷⁷ The court entered default judgment against Morgan Stanley, leaving only the question of damages for a jury, which awarded Coleman Holdings \$1.45 billion.⁷⁸ While the judgment, including the award of punitive damages, was later reversed on grounds unrelated

⁷² Sarah Michaels Montgomery, *E-discovery: Aligning Practice with Principles*, THE SCITECH LAWYER, Fall 2007, at 12.

⁷³ Coleman Holdings v. Morgan Stanley & Co., 2005 Extra LEXIS 94 (Fla. Cir. Ct. Mar. 23, 2005). The court found that Morgan Stanley made misrepresentations in a court-ordered "Certificate of Compliance," failed to properly account for "newly discovered" network backup tapes, failed to produce attachments to e-mails, and failed to properly perform electronic text searches when looking for responsive documents.

⁷⁴ Id. at *4.

⁷⁵ Id. at *8

⁷⁶ Id. at *14-15.

⁷⁷ Id. at *15.

⁷⁸ Id. at *33-34.

COUGHLIN DUFFY LLP

to the electronic discovery issues (which were not discussed by the appellate court), the trial court's rulings and the jury's findings serve as a good example of the potential impact of electronic discovery abuses.

In the leading case of Zubulake v. UBS Warburg,⁷⁹ the court imposed sanctions against UBS Warburg and admonished counsel and client by quoting the classic line from the movie *Cool Hand Luke*, "What we've got here is a failure to communicate." The court spoke at length on the need for counsel to interface extensively with IT personnel to "become fully familiar with her client's . . . data retention architecture," and emphasized that counsel and client's failure to do so played a large role in the sanctions that ultimately led to the \$29 million verdict against the investment firm.

In a more recent case between Qualcomm and Broadcom, communications companies involved in a patent infringement litigation, a judge ordered Qualcomm to pay Broadcom's attorney's fees of \$8.5 million. At trial, a witness revealed the existence of 21 e-mails that had not been produced by Qualcomm. The revelation led to the discovery of hundreds of thousands of relevant documents that had not been produced. Significantly, an attorney for Qualcomm falsely gave the judge the impression that he was unaware of the 21 e-mails. After Broadcom prevailed at trial, the judge ordered that Qualcomm should also pay Broadcom's attorney's fees.⁸⁰ A decision has not been made on what, if any, sanctions will be imposed on the attorneys for Qualcomm.⁸¹

The most severe sanctions are imposed when there has been spoliation of evidence. Spoliation of evidence is the destruction or significant alternation of evidence, or the failure to

⁷⁹ Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004) ("Zubulake V").

⁸⁰ Jessie Seyfer, *Judge: Qualcomm Firms Can Disclose Work Product*, THE RECORDER, October 1, 2007, [available at www.law.com](http://www.law.com).

⁸¹ Jessie Seyfer, *Day Casebeer Partner Is Central to Qualcomm Discovery Mess*, THE RECORDER, October 4, 2007, [available at www.law.com](http://www.law.com).

COUGHLIN DUFFY LLP

preserve property for another's use as evidence in pending or reasonably foreseeable litigation.⁸² The consequences of spoliation are seen in the Morgan Stanley and Zubulake cases. In Thompson v. United States Department of Housing and Urban Development,⁸³ a class action suit alleging racial discrimination in urban housing, the court noted that the Rules allow for such "draconian" sanctions that are often "case determinative."⁸⁴ In that case, the plaintiffs sought to bar the calling of witnesses whose e-mails had not been produced by the defendant.⁸⁵ The court noted that, after finding that spoliation had occurred, it is left to the court's discretion what sanctions to impose.⁸⁶

Where spoliation is egregious, courts will impose an adverse inference that can be used against the wrongdoer at trial. A party seeking an adverse inference based on spoliation must establish: (1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed 'with a culpable state of mind'; and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense."⁸⁷

In Jane Doe v. Norwalk Community College,⁸⁸ a Connecticut community school was sanctioned for discovery misconduct and spoliation of evidence for its destruction of electronic data. The plaintiff in this gender discrimination case sought an adverse inference against the defendant for completely erasing the hard drives of key witnesses.⁸⁹ The court allowed an adverse inference against the school at trial, specifically, the presumption that the destroyed

⁸² Mosaid Technologies, Inc. v. Samsung Elecs. Co., Ltd., 348 F. Supp. 2d 332, 335 (D.N.J. 2004) (citing Zubulake V, 229 F.R.D. at 430).

⁸³ 219 F.R.D. 93 (D. Md., December 12, 2003).

⁸⁴ Id. at 102.

⁸⁵ Id. at 96.

⁸⁶ Id. at 100.

⁸⁷ Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 107 (2d Cir. 2002).

⁸⁸ 2007 U.S. Dist. LEXIS 51804 (D.Conn., July 16, 2007),

⁸⁹ Id. at *5.

COUGHLIN DUFFY LLP

evidence was unfavorable to the school's defense, and awarded the costs of the motion to the plaintiff.⁹⁰

Other options are also available to courts. Recently, a district court in the District of Columbia ordered the solicitation of bids from forensic computer technicians to assess whether the search and restoration of additional data from defendant's company computer was justified under F.R.C.P. 26(b)(2)(c).⁹¹ In Peskoff v. Faber, the plaintiff sought e-mails received or authored by him, which the defendant claimed no longer existed.⁹² Despite the fact that there was an archive of all electronic documents on the plaintiff's hard drive at the time he left the defendant's company, the defendant claimed that no e-mails existed for a two year period.⁹³ Because this time period pre-dated the litigation, the court found that the defendant was not obliged to preserve those documents.⁹⁴ There was no doubt that the information sought was relevant, and the court determined that a forensic search of the defendant's computers was in order, to ascertain what, if anything, remained.⁹⁵

Court's have imposed an expansive net over a party's obligation to preserve responsive ESI and an adversary's access to same. This does not mean that a party has unfettered access to his adversary's electronic databases. In fact, courts have held that the Rules generally do not give the requesting party the right to search the responding party's records.⁹⁶ Notwithstanding, the above examples illustrate the importance of developing reliable resources to navigate the corporate infrastructure, as well as the risks associated with "going it alone" or, even worse,

⁹⁰ Id. at *30.

⁹¹ Peskoff v. Faber, 2007 U.S. Dist. LEXIS 62595 (D.D.C. August 27, 2007).

⁹² Id. at *1-2.

⁹³ Id. at *2.

⁹⁴ Id. at *21.

⁹⁵ Id. at *25.

⁹⁶ In Re Ford Motor Co., 345 F.3d 1314, 1317 (11th Cir. 2003); see also Butler v. Kmart Corporation, 2007 WL 240682 (N.D. Miss., Aug. 20, 2007) (stating that the 2006 amendments to the Federal Rules of Civil Procedure concerning electronically stored information do not disturb the validity of In Re Ford Motor Co.).

going with the wrong person. The same lesson is imparted by the changing rules, as federal and state rules of procedure require the identification of a contact person with extensive knowledge of IT systems to assist in coordinating discovery.

V. Best Practices Guidelines for E-Discovery

A. The Role of the Document Retention and E-mail Retention Policy

Now that the Rules explicitly include ESI, the distinction, or lack thereof, between "document" and "data" must likewise be addressed in corporate document retention policies. In the past, some organizations may have found such policies unnecessary. However, considering the sheer volume of data passing through most worldwide organizations, it is prudent to address data retention practices and formalize a written policy. In fact, in making a determination whether there has been "spoliation" or a "good-faith operation of an electronic information system," a court may examine the document/data retention policy in effect at the time.⁹⁷ For example, in Arthur Andersen LLP v. United States, the United States Supreme Court addressed the document retention practices of Arthur Andersen during the Enron investigation.⁹⁸ The accounting firm's policy, even after the recognition of an impending investigation and litigation, allowed for the destruction of documents that could be relevant.⁹⁹ In that case, the continued destruction of documents in the face of knowledge of an impending investigation and litigation led to the criminal indictment of Arthur Andersen.¹⁰⁰

While most cases will not lead to criminal liability, Arthur Andersen, LLP illustrates the dangers that abound when companies do not give the proper attention to their document retention

⁹⁷ Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005); see also Samsung Elecs. Co. v. Rambus Inc., 439 F. Supp. 2d 524 (E.D. Va. 2006); Hynix Semiconductor, Inc. v. Rambus, Inc., 2006 U.S. Dist. LEXIS 30690, 2006 WL 565893, *20 (N.D. Cal. 2006).

⁹⁸ Arthur Andersen LLP, 544 U.S. at 699-700.

⁹⁹ Id. at 700-01.

¹⁰⁰ Id. at 702.

COUGHLIN DUFFY LLP

programs. Rule 37(f) explicitly requires courts to analyze whether the loss or alteration of ESI occurred as the result of "routine, good-faith operation" of the system. While this language allows a company to continue using its normal procedures, absent notice of impending litigation, it does not absolve companies from being watchful for signs that they may become embroiled in litigation. Significantly, this safe-harbor provision under Rule 37(f) does not relieve a party from sanctions for the loss or alteration of evidence which occurred pursuant to a retention policy.

Therefore, it is of critical importance for companies to understand how each of their systems manages and ultimately deletes data. Without an understanding of the infrastructure and internal operating system, a party may find itself unable to create, update and implement an effective policy. Competing interests between the IT and legal professionals can be expected. Therefore, an organization's legal team and IT professionals must work together in the creation or updating of a policy and, more importantly, in its ultimate implementation. IT staff responsible for implementing document retention policies with respect to ESI may not even be aware that there is an obligation to preserve ESI that they destroy on a routine periodic basis. Failure to notify responsible IT staff of what ESI must be preserved so that ESI is not destroyed could subject a company to sanctions.¹⁰¹

For example, it is common for network and server accounts to be disabled; e-mail accounts to be disabled; and voice mail accounts to be deactivated when an employee leaves an organization. Sometimes the disabling of these accounts will result in, or be accompanied by, destruction of ESI associated with those accounts. Individual PCs may be "recycled" and reissued to another employee or even disposed of and all the ESI on the PC may be destroyed as a result. Importantly, ESI, unlike physical records, is also subject to automatic destruction without any explicit action. Network and computer log files are usually limited by time or size

¹⁰¹ Kier v. UnumProvident Corp., 2003 U.S. Dist. LEXIS 14522 (S.D.N.Y. Aug. 22, 2003).

COUGHLIN DUFFY LLP

so that new activity overwrites old activity. There may be a need to suspend the automatic destruction of ESI so that discoverable ESI that is subject to preservation obligations is not inadvertently destroyed.

Remember that a document retention policy tells a story that may be subject to the scrutiny of hindsight in the event that information that once existed is unavailable during litigation or other legal proceedings. Therefore, the policy should accomplish at least four goals: (1) identify subject documents; (2) embody legal objectives; (3) identify specific time periods for retention; and (4) explain processes and lines of responsibility in clear unambiguous terms. More importantly, the policy must be realistic and enforced. However, merely having a policy in place will not provide a safe-harbor to an organization that may be faced with discovery sanctions. In this context, an organization will have to demonstrate its good-faith operation of an electronic information system, that a well-reasoned document retention policy is in place and that all persons relevant to its enforcement are properly trained.

The document retention policy is a double-edged sword in that its proper creation and implementation can protect a party from sanctions; but an ill-advised policy or one not properly followed can, in fact, create the record to support a claim of failure to act "in good faith." In this regard, the most important aspect of the policy is the section that provides for suspension of that very policy, the litigation hold or preservation notice. Although at first glance companies may not want to expend the effort and resources on amending or adopting a document retention policy that anticipates a litigation hold, it is undoubtedly worth the effort when compared to the ramifications of not doing so.

B. E-Discovery Liaison

Soon after litigation has begun, parties will begin exchanging discovery, including ESI.¹⁰² Federal courts expect parties to work amongst themselves and agree about what ESI will be turned over, and in what form. As stated above, the Rules now requires parties to identify and resolve differences related to disclosure or discovery of ESI (including format of production) in advance of the initial conference with a judge that results in a discovery scheduling order. Each party should appoint an e-discovery liaison, through whom all e-discovery requests and responses are channeled.¹⁰³

An “e-discovery liaison” is an individual through whom all e-discovery requests and responses are channeled.¹⁰⁴ The liaison can be an employee, an attorney or a third party consultant, and should know the systems a party uses, as well as the mechanics of e-discovery.¹⁰⁵ Besides organizing a party’s e-discovery, the liaison should also be able to participate in e-discovery dispute resolutions.¹⁰⁶ Many states have codified similar procedures within their rules, and some courts, such as the U.S. District Court for the District of New Jersey, go further by requiring parties to identify an “e-discovery liaison” to assist counsel in the preliminary stages leading up to the initial conference with the court.¹⁰⁷ Although not mandated by the federal rules, companies should seriously consider the implementation of this role before the next lawsuit arises.

One of the biggest issues with which a liaison is a benefit is determining precisely what must be turned over. Besides concerns over whether various evidentiary privileges may apply to

¹⁰² F.R.C.P. 26(a)(2006), F.R.C.P. 26(a)(2007).

¹⁰³ Model Order Governing the Exchange of Electronic Discovery, District Court for the Eastern District of Pennsylvania, available at www.paed.uscourts.gov/documents/procedures/savpol6.pdf.

¹⁰⁴ Id.

¹⁰⁵ Id.

¹⁰⁶ Id.

¹⁰⁷ District of New Jersey Local Rule 26.1(d)(1).

COUGHLIN DUFFY LLP

prevent the disclosure of some information, in the digital age, parties are also concerned about the form of ESI to be turned over. For example, a party may wish to turn over a hard copy (print out) of ESI, but doing so obscures some of the data contained in the digital form, such as a spreadsheet. Can a party turn over the hard copy, or must it turn over the digital file? And if it must turn over the digital file, can it make any alterations to the data before turning it over? Must it obtain permission from the court before doing so?

The selection of the individual for this role should be thought out and not merely a “front person.” First, the liaison should be knowledgeable enough to present an inventory of the active corporate systems that store and manage all information, as well as obsolete (legacy) systems, backup and archive media for the time period that counsel deems relevant. In addition, there should be a discussion of network or system “settings” that affect storage and deletion of data, such as dated e-mails and attachments. The extent to which settings are changed, even if such changes increase costs, should be a dialogue with consideration of legal and other business concerns.

Some consideration should be given to the liaison's effectiveness as a witness. As discovery focuses more on technology, a subject alien to many attorneys and judges, the quality and quantitative depth of the individual explaining such issues will influence the success rate of the litigation. It is worth noting here that a trend is developing where courts are suggesting that counsel be accompanied by IT professionals when meeting with adversaries and/or the court to resolve discovery disputes, even if the input from the professional is provided off the record, confidentially or *in camera*.

Finally, it is important to recognize that the creation of a reliable contact or network of contacts within the IT ranks is neither a distraction nor an added expense. If properly prepared

and engaged, the e-discovery liaison is an investment in an enduring resource that is likely to yield substantial economic returns by reducing litigation costs and exposure. Even better, the institutionalization of electronic discovery resources and a litigation response plan will reap greater benefit with cases, as storage and processes are streamlined and data are reused (and already authenticated) when overlapping facts arise in separate suits. Perhaps the best benefit of all is that the company will be prepared, and its processes will be defensible.

VI. Conclusion

While modern companies face daunting challenges when managing their ESI, successful administration of electronic systems can be achieved with proper preparation. The examples of sanctions and large judgments in this paper are reminders of what happens to companies that do not properly consider potential litigation when designing their document retention systems. Corporations must form a working group made up of executives, attorneys and representatives of the IT department. This working group should create a document retention policy to disseminate to all employees. The policy must outline situations and events which could lead to potential litigation. It should inform all employees that they should report such events to a member of the working group. The policy should include procedures for putting a litigation hold on ESI which may be relevant in any possible litigation, including what computer systems will be used to store information which would otherwise be deleted in the normal course of business. The policy should also provide guidance on how to proceed once a complaint has been filed, including the identification of “key players” and relevant documents. The policy should indicate what procedures will be used for the production of ESI, the formation of any agreements about production with other parties in litigation, and what forms of ESI should be requested from other parties.

COUGHLIN DUFFY LLP

It goes without saying that litigation is an expensive prospect for any organization, small or large. However, with the right policies and procedures in place, companies can greatly reduce the likelihood of large sanctions or judgments. Accordingly, we strongly recommend that you carefully review your policies, procedures and practices regarding electronic data. E-discovery issues arise in every case. The difficulty and daunting challenges emerge in determining how to deal with the issues in cases that have varying fact patterns and varying amounts in controversy. Importantly, organizations need to overcome the “language barrier” between IT and legal that occurs from the discussion of technical issues. There must be a proper understanding of the obligation of preserving electronic data in anticipated or pending litigation or regulatory investigation. An important factor for organizations is to learn to manage the rising costs of electronic discovery including the design of an electronic data strategy for responding to discovery requests which include narrowing the scope to relevant data; avoiding undue burden or expense; and seeking cost shifting as appropriate. Finally, and most importantly, businesses must develop best practices in dealing with the emerging and changing issues of electronic discovery.